API 网关

用户指南

发布日期　2023-05-30

目 录

1 产品介绍.....1
1.1 什么是 API 网关.....1
1.2 产品优势.....2
1.3 应用场景.....3
1.4 产品规格差异.....4
1.5 约束与限制.....5
1.6 权限管理.....6
1.7 基本概念.....8
1.8 计费说明.....10
2 快速入门.....11
2.1 概述.....11
2.2 开放 API.....11
2.2.1 开放 API 流程.....11
2.2.2 创建 API 分组.....13
2.2.3 绑定域名.....13
2.2.4 创建 API.....14
2.2.5 调试 API.....16
2.2.6 创建环境（可选）.....17
2.2.7 发布 API.....17
2.3 调用 API.....18
2.3.1 调用 API 流程.....18
2.3.2 创建凭据并获取授权.....19
2.3.3 为简易认证添加 AppCode.....19
2.3.4 调用 API.....20
3 新旧版本差异.....21
4 总览.....23
5 API 管理.....27
5.1 创建 API 分组.....27
5.2 绑定域名.....29
5.3 创建环境变量.....30
5.4 新增网关响应.....31
5.5 创建 API.....33

5.6 开启跨域访问.....46
5.7 调试 API.....52
5.8 授权 API.....52
5.9 发布 API.....53
5.10 下线 API.....54
5.11 导入 API.....55
5.12 导出 API.....56
5.13 查看 API 列表.....57
5.14 支持 HTTP2.0.....57
6 API 策略.....58
6.1 创建策略.....58
6.2 跨域资源共享策略说明.....60
6.3 HTTP 响应头管理策略说明.....62
6.4 流量控制 2.0 策略说明.....64
6.5 Kafka 日志推送策略说明.....67
6.6 断路器策略说明.....69
6.7 流量控制策略说明.....75
6.8 访问控制策略说明.....77
6.9 签名密钥策略说明.....78
6.10 自定义认证.....79
6.11 SSL 证书管理.....81
6.12 负载通道.....83
6.13 环境管理.....86
7 凭据管理.....88
7.1 创建凭据并绑定 API.....88
7.2 重置 Secret.....89
7.3 为简易认证绑定 AppCode.....89
7.4 绑定凭据配额策略.....90
7.5 绑定访问控制策略.....91
8 监控分析.....93
8.1 API 监控.....93
8.1.1 支持的监控指标.....93
8.1.2 创建告警规则.....95
8.1.3 查看监控指标.....96
8.2 日志分析.....96
9 实例管理.....100
9.1 购买实例.....100
9.2 查看或编辑实例信息.....103
9.3 配置参数.....104
10 SDK.....106

11 调用已发布的 API 107
11.1 调用 API 107
11.2 响应消息头 109
11.3 错误码 109
12 权限管理 114
12.1 创建用户并授权使用 API 网关 114
12.2 API 网关自定义策略 115
13 云审计服务支持的关键操作 117
13.1 云审计服务支持的 APIG 操作列表 117
13.2 查看云审计日志 120
14 常见问题 121
14.1 热门咨询 121
14.2 API 创建 122
14.2.1 无法创建 API 是什么原因？ 122
14.2.2 API 的响应码如何定义？ 122
14.2.3 使用 VPC 通道（负载通道），后端服务的主机端口怎么填写？ 122
14.2.4 不使用 VPC 通道（负载通道）时，后端服务地址可以是什么？ 122
14.2.5 后端服务地址是否一定要配置为 ECS 的地址？ 122
14.2.6 后端服务是否支持绑定私网 ELB 地址？ 122
14.2.7 后端服务地址可以填写私有地址（子网 IP）吗？ 122
14.2.8 API 网关是否支持多后端节点方案？ 123
14.2.9 独立域名申请后还需要做什么？ 123
14.2.10 API 网关可以绑定内网域名吗？ 123
14.2.11 为什么分组跨域配置失败？ 123
14.3 API 调用 124
14.3.1 API 调用失败的可能原因有哪些？ 124
14.3.2 API 调用返回错误码如何处理？ 125
14.3.3 API 调用报错“414 Request-URI Too Large” 125
14.3.4 "The API does not exist or has not been published in the environment."如何解决？ 125
14.3.5 No backend available，怎么解决？ 125
14.3.6 后端服务调用失败“Backend unavailable”或超时“Backend timeout”原因分析 125
14.3.7 后端服务调用报错域名无法解析“Backend domain name resolution failed” 126
14.3.8 修改后端服务的超时时间上限“backend_timeout”后未生效 128
14.3.9 如何切换调用环境？ 128
14.3.10 调用请求包最大支持多少？ 128
14.3.11 使用 iOS 系统时，如何进行 APP 认证？ 128
14.3.12 新建一个 IAM 认证方式的 API，在配置入参时为什么无法配置 HEADER 位置的 x-auth-token？ 128
14.3.13 凭据问题汇总 128
14.3.14 是否支持移动应用调用 API？ 129
14.3.15 部署在 VPC 下的应用是否可以调用 API？ 129
14.3.16 如何实现 WebSocket 数据传输？ 130

14.3.17 API 调用是否支持长连接 130
14.3.18 策略后端有多个时，怎么匹配和执行 130
14.3.19 API 调用对请求的响应消息体限制 130
14.3.20 如何通过 APIG 访问公网后端服务 131
14.4 API 认证鉴权 131
14.4.1 是否支持 HTTPS 的双向认证？ 131
14.4.2 “无认证”方式的 API 该怎么鉴权与调用？ 131
14.4.3 TLS 加密协议支持什么版本？ 131
14.4.4 API 签名认证能否自定义鉴权方式？ 131
14.4.5 安全认证签名的内容是否包括 Body 体 131
14.4.6 IAM 认证信息错误 131
14.5 API 控制策略 134
14.5.1 API 流量控制 134
14.5.1.1 是否支持对请求并发次数做自定义控制？ 134
14.5.1.2 每个子域名（调试域名）每天最多可以访问 1000 次，如果帐号为企业帐号，是否还有这个限制？ 134
14.5.1.3 API 调用是否存在带宽限制 135
14.5.1.4 流量控制策略不生效怎么办？ 135
14.5.2 API 访问控制 135
14.5.2.1 怎样给指定的用户开放 API 135
14.5.2.2 配置了身份认证的 API，如何在特殊场景下（如指定 IP 地址）允许不校验身份？ 135
14.6 API 发布 135
14.6.1 对 API 的修改是否需要重新发布？ 135
14.6.2 API 发布到 RELEASE 环境可以正常访问，发布到非 RELEASE 环境无法访问？ 135
14.6.3 API 发布到不同环境后，会调用不同的后端服务吗？ 136
14.6.4 API 调试的时候，如何指定环境？ 136
14.7 API 导入导出 136
14.7.1 API 导入失败是什么原因？ 136
14.7.2 swagger 导入 API 的扩展字段有没有模板？ 136
14.8 API 安全 136
14.8.1 怎样保护 API？ 136
14.8.2 怎样保证 API 网关调用后端服务器的安全？ 136
14.8.3 能否针对 VPC 通道（负载通道）内的 ECS 私有 IP 进行访问控制 137
14.9 其他 137
14.9.1 API、环境、凭据之间的关系？ 137
14.9.2 怎样使用 API 网关？ 137
14.9.3 API 网关支持哪些 SDK 语言？ 137
14.9.4 API 网关是否支持通过 POST 方法上传文件？ 138
14.9.5 如何获取 API 网关错误返回信息？ 138
14.9.6 API 网关是否支持部署到本地？ 138
15 修订记录 139

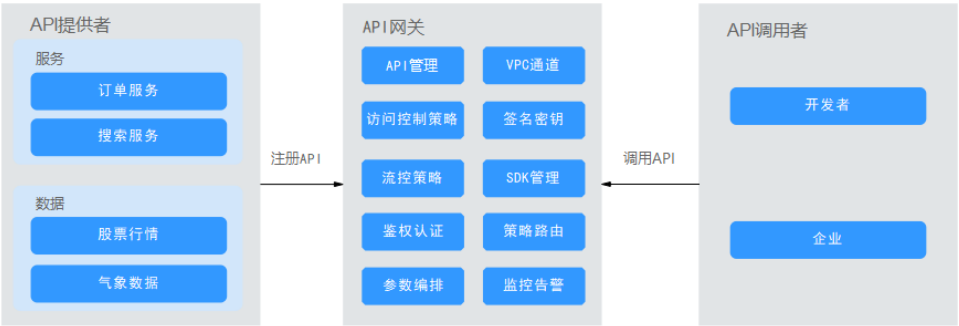
1 产品介绍

1.1 什么是 API 网关

API网关（API Gateway）提供高性能、高可用、高安全的API托管服务，能快速将企业服务能力包装成标准API接口，帮助您轻松构建、管理和部署任意规模的API。借助API网关，可以简单、快速、低成本、低风险地实现内部系统集成和业务能力开放。

- 如果您作为API提供者，您可以将成熟的业务能力（如服务、数据等）作为后端服务，在API网关中开放API，并通过线下方式提供给API调用者使用，实现业务能力变现。
- 如果您作为API调用者，您可以获取并调用API提供者在API网关开放的API，减少开发时间与成本。

图 1-1 API 网关服务简介



产品功能

- **API生命周期管理**

  包括API的创建、发布、下线和删除的完整生命周期管理功能。通过API生命周期管理功能，您可以快速、高效的开放成熟的业务能力。

- **便捷调试工具**

  API网关提供页面调试工具，您可以使用该工具添加HTTP头部参数与body体参数，对API进行调试，简化API开发，降低API的开发维护成本。

- **版本管理**

API可以发布到不同的环境，如果您需要再次发布此API到之前已发布的环境，那么此次的发布版本将立即覆盖之前的版本。API网关支持查看API发布历史（如版本、发布说明、发布时间和发布环境），并支持回滚到任一API历史版本，以便满足业务灰度发布、版本升级、回滚等需求。

- **环境变量**

  环境变量是指在环境上创建可管理的一种变量，该变量固定在环境上。当API发布到不同环境时，发布过程中变量标识会被相应环境的变量值替换，API本身定义不变。通过创建环境变量，实现同一个API，在不同环境中调用不同的后端服务。

- **精细流量控制**
  - 针对不同的业务等级、用户等级，可实施API的请求频率、用户的请求频率、凭据的请求频率和源IP的请求频率的管控，用于保障后端服务的稳定运行。
  - 针对API调用path、query、header等参数精细化配置不同的流量的限制。
  - 流量控制的时间单位可以是秒、分钟、小时或天。
  - 针对特殊的应用和租户设置特殊的流控限制。

- **监控告警**

  提供实时、可视化的API监控，包括：API请求次数、API调用延迟和API错误信息，通过监控面板更清晰地了解API的调用情况，识别可能影响业务的潜在风险。

- **安全防护**
  - 域名访问认证支持TLS1.1、TLS1.2防护。
  - 访问控制策略主要用来控制访问API的IP地址和帐户，您可以通过设置IP地址或帐户的黑白名单来拒绝/允许某个IP地址或帐户访问API。
  - 断路器策略是API网关在后端服务出现性能问题时保护系统的机制，支持通过熔断降级的方式保护后端服务。
  - 身份认证策略支持通过AKSK、Token等多种方式进行服务认证，支持用户通过函数自定义API访问认证逻辑，支持对后端服务进行证书校验，支持签名密钥用于后端服务验证API网关的身份。

- **负载通道**

  在API网关中创建负载通道来访问VPC环境中的资源，并将部署在VPC中的后端服务开放为API。负载通道具有负载均衡功能。

- **模拟响应**

  API网关支持设置模拟的API后端响应，支持利用Mock响应支持熔断降级、重定向等场景。

1.2 产品优势

开箱即用的服务

只需在管理控制台配置，即可快速创建API。提供页面调试工具，简化API开发。可同时发布一个API到多个环境，快速迭代、测试API。

便捷的 API 生命周期管理

API网关提供全生命周期的API管理，从设计、开发、测试、发布、运维等， 实现完整的API解决方案。帮助您轻松构建、管理和部署任意规模的API。

精细化秒级流控

API网关采用同步加异步混合流控的方式，通过多种算法，实现精细化的秒级流控。同时提供灵活自定义的流量控制策略制定，保障API服务的稳定和连续。

支持函数直接调用

与函数工作流服务无缝对接，支持将函数工作流服务以API形式开放使用。

可视化 API 监控面板

帮助您监控API调用性能指标、数据延迟以及错误等信息，识别可能影响业务的潜在风险。

多层安全防护

API网关具备SSL传输、严格的访问控制、IP黑白名单控制、认证鉴权、防重放防攻击、多种审计等安全措施，全方位保护API安全调用，且能实施灵活而精细的配额管理及流控管理以保护您的后端服务。帮助您灵活、安全的开放您的服务。

灵活的策略路由

支持配置不同的后端，按照多种策略进行匹配转发，轻松解决企业应用的灰度发布，环境管理等难题。

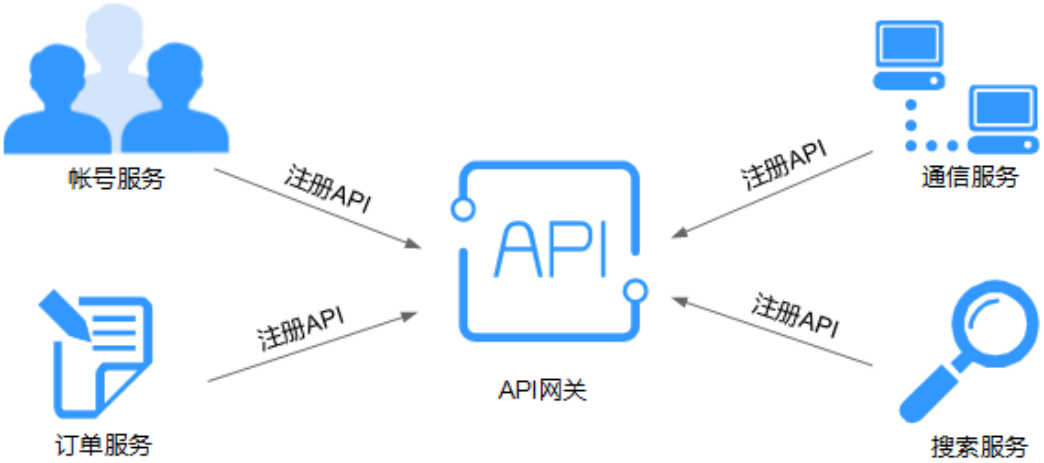
多语言 SDK

API网关为客户端提供Java、Go、Python、C等多语言的SDK接入，业务后端无需做修改，轻松实现一套系统对接多种业务场景（如移动场景、IoT场景等）。

1.3 应用场景

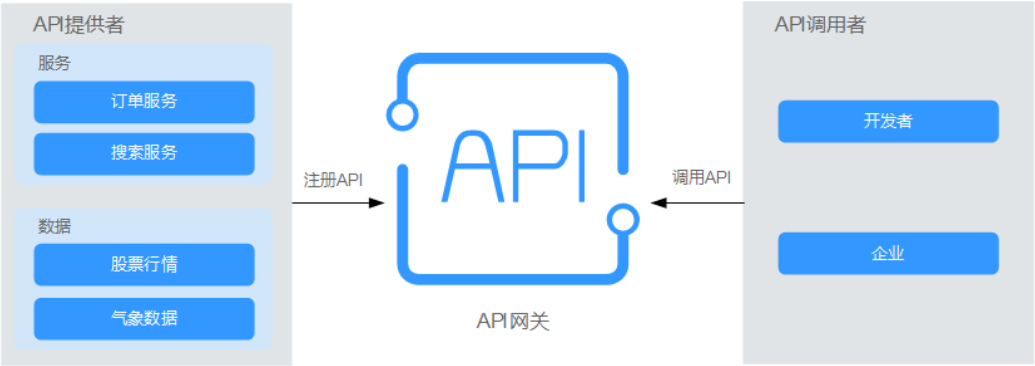
企业内部系统解耦

随着企业的高速发展、业务的快速变化，需要企业内部系统跟随业务需求一同变化，但是企业内部系统存在相互依赖关系，为保持系统的通用性与稳定性，很难应对业务的变化。而API网关使用RESTful API， 帮您简化服务架构，通过规范化、标准化的API接口，快速完成企业内部系统的解耦及前后端分离。同时，复用已有能力，避免重复开发造成的资源浪费。



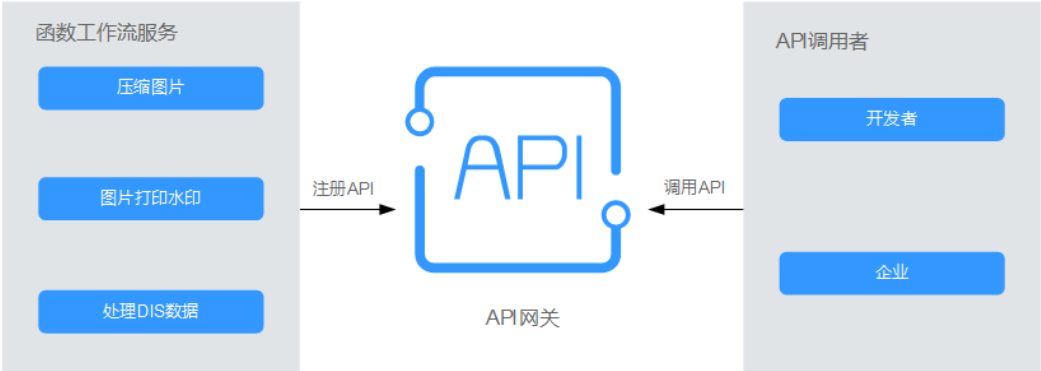
企业能力开放

当今企业面临巨大的挑战，企业的发展需要依赖外部合作伙伴的能力，典型的例子如使用第三方平台支付、合作方帐户登录等。通过API网关将企业内部服务能力以标准API的形式开放给合作伙伴，与合作伙伴共享服务和数据，达成深度合作，构建企业共赢生态。



函数工作流服务开放

API网关可以将无服务器服务（即函数工作流服务）作为后端服务开放给合作伙伴，与传统的服务相比，函数工作流服务具有易开发、易部署、易维护的特点。使用函数工作流服务，快速构建后端业务逻辑处理，将这些业务逻辑函数通过API网关的标准API接口开放，并发能力得到线性扩展。



1.4 产品规格差异

专享版规格

APIG专享版实例规格说明如**表1-1**所示。

表 1-1 专享版实例规格说明

实例规格	每秒最大请求数
基础版	2000
专业版	4000

实例规格	每秒最大请求数
企业版	6000
铂金版	10000

说明

- 专享版的“每个API的访问频率”可调整上限，参考配置为上表所列出的每秒最大请求数。
- 目前不支持修改专享版实例规格。
- 专享版实例规格为在以下条件中测试得出：
  - 连接协议：https
  - 连接类型：长连接
  - 并发数：100
  - 认证方式：无认证
  - 返回数据大小：1KB
  - 带宽：10MB

1.5 约束与限制

如果您需要修改默认限制值，请参考“帮助中心 > 其他 > 常见问题 > 如何申请扩大配额”。

须知

新增或修改的APIG资源存在数据同步延迟，需要5-10秒才生效。

表 1-2 专享版 API 网关配额管理明细

限制项	默认限制	能否修改
实例数量	每个用户最多创建5个实例。	√
API分组数量	每个实例最多创建1500个API分组。	√
API数量	每个实例： ● 基础版：250 ● 专业版：800 ● 企业版：2000 ● 铂金版：8000	√
后端策略数量	每个实例最多创建5个后端策略。	√
凭据数量	每个实例最多创建50个凭据。凭据配额包括用户自行创建的凭据。	√

限制项	默认限制	能否修改
流控策略数量	● 每个实例最多创建300个流控策略。 ● 用户流量限制不超过API流量限制。 ● 凭据流量限制不超过用户流量限制。 ● 源IP流量限制不超过API流量限制。	√
环境数量	每个实例最多创建10个环境。	√
签名密钥数量	每个实例最多创建200个签名密钥。	√
访问控制策略数量	每个实例最多可以创建100个访问控制策略。	√
VPC通道（负载通道）数量	每个实例最多创建200个VPC通道。	√
变量数量	每个分组在任意一个环境中，最多创建50个变量。	√
独立域名数量	每个分组最多可以绑定5个独立域名。	√
云服务器数量	每个VPC通道最多添加10个云服务器。	√
参数数量	每个API最多创建50个参数。	√
发布历史数量	同一个API在每个环境中最多记录10条最新的发布历史。	√
每个API的访问频率	不超过6000次/秒。	√
特殊应用	每个流控策略最多可创建30个特殊应用。	√
特殊租户	每个流控策略最多可创建30个特殊租户。	√
子域名（调试域名）访问次数	每个子域名每天最多可以访问1000次。	x
调用请求包的大小	API每次最大可以调用12M的请求包。	√
TLS协议	支持TLS1.1和TLS1.2，推荐使用TLS1.2。	√
自定义认证数量	每个实例最多创建50个自定义认证。	x
插件数量	每个实例最多创建500个插件。	√

1.6 权限管理

如果您需要对云上购买的API网关（API Gateway）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity

and Access Management，简称IAM ）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云资源的访问。

通过IAM，您可以在云帐号中给员工创建IAM用户，并使用策略来控制员工对API网关资源的访问范围。

如果云帐号已经能满足您的需求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用API网关服务的其它功能。

API 网关系统角色

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

API网关服务部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问API网关服务时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略，策略是角色的升级版。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对API网关服务，管理员能够控制IAM用户进行指定的管理操作。权限策略以API接口为粒度进行权限拆分，API网关服务支持的API授权项请参见《API网关接口参考》中“权限策略和授权项”章节。

如表1-3所示，包括了API网关的所有系统角色和策略。

表 1-3 API 网关的系统角色或策略

系统角色/策略名称	描述	类别	依赖关系
APIG Administrator	API网关服务的管理员权限。拥有该权限的用户可以使用API网关服务的所有功能。	系统角色	无。
APIG FullAccess	API网关服务所有权限。拥有该权限的用户可以使用**专享版**API网关服务的所有功能。	系统策略	无。
APIG ReadOnly Access	API网关服务的只读访问权限。拥有该权限的用户只能查看**专享版**API网关的各类信息。	系统策略	无。

以上系统角色或策略的具体权限内容，可以从IAM服务控制台查看。例如APIG FullAccess的策略内容为：

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "apig:*:*",
            "vpc:*:get*",
            "vpc:*:list*",
            "vpc:ports:create",
            "vpc:ports:update",
            "vpc:ports:delete",
            "vpc:publicIps:update",
            "FunctionGraph:function:listVersion",
            "FunctionGraph:function:list",
            "FunctionGraph:function:getConfig",
            "ecs:servers:list",
            "lts:groups:list",
            "lts:logs:list",
            "lts:topics:list"
         ],
         "Effect": "Allow"
      }
   ]
}
```

相关文档

- 《统一身份认证服务用户指南》中“产品简介”章节
- 《API网关用户指南》中“创建用户并授权使用API网关”章节

1.7 基本概念

API

API（Application Programming Interface，应用程序编程接口）是一些预先定义的函数，应用将自身的服务能力封装成API，并通过API网关开放给用户调用。

API包括基本信息、前后端的请求路径和参数以及请求相关协议。

API 分组

API分组是同一种业务API的集合，API开发者以API分组为单位，管理分组内的所有API。

环境

为了方便管理API的生命周期，API网关定义了API受限使用范围，这个受限使用的范围，称为环境，例如API的测试环境，开发环境等。

环境定义了API生命周期管理过程中的不同状态，API可以被发布到不同的自定义环境中。

调用不同环境的API，一般通过在API调用的请求头增加指定的头部参数，头部参数名固定为x-stage，它的取值叫环境名，用以区分不同的环境。

环境变量

在环境上创建可管理的一种变量，该变量固定在环境上。通过创建环境变量，实现同一个API，在不同环境中调用不同的后端服务。

流量控制

流量控制支持从用户、凭据、源IP和时间段等不同的维度限制对API的调用次数，保护后端服务。

API网关支持按分/按秒粒度级别的流量控制。

访问控制

访问控制策略是API网关提供的API安全防护组件之一，主要用来控制访问API的IP地址和帐户，您可以通过设置IP地址或帐户的黑白名单来允许/拒绝某个IP地址或帐户访问API。

凭据

凭据定义了一个API调用者的身份。可以将一个API授权给多个凭据，也可以将多个API授权给同一个凭据。

签名密钥

签名密钥由一对Key和Secret组成，用于后端服务验证API网关的身份，在API网关请求后端服务时，保障后端服务的安全。

当签名密钥绑定API后，API网关向后端服务发送此API的请求时，会增加相应的签名信息，此时后端服务依照同样方式进行签名并得到签名结果，如果和API网关传过来的Authorization头中签名一致，则可证明API请求确实来自API网关，而不是其他伪造请求。

负载通道

API网关通过负载通道访问部署在VPC内的服务，您可以借助API网关将部署在VPC中的后端服务开放给第三方用户调用。

自定义认证

自定义认证指在API调用过程中，用户可自行定义认证规则，实现API网关对调用方发起的请求、后端服务对API网关转发的请求进行有效性以及完整性校验。

自定义认证包含以下两种认证：

- 前端自定义认证：如果您希望使用自己的认证系统，而不是APP认证/IAM认证对API的访问进行认证鉴权时，您可以使用自定义认证，通过您自定义的函数进行认证鉴权。
- 后端自定义认证：当不同的后端服务使用不同的认证系统时，导致您需要为不同的认证系统定制化开发API，而APIG通过自定义认证功能，将多种认证系统集成，简化API开发的复杂度。您只需要在APIG中创建自定义的函数认证，APIG通过此函数对接后端认证系统，获取后端服务的访问授权。

简易认证

简易认证指调用API时，在HTTP请求头部消息增加一个参数X-Apig-AppCode（参数值填AppCode），而不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。

网关响应

网关响应指API网关未能成功处理API请求，从而产生的错误响应。API网关提供默认的网关响应（default），如果您需要自定义响应状态码或网关响应内容，可在API分组管理中新增网关响应，其中响应内容符合JSON格式即可。

1.8 计费说明

API网关（API Gateway）帮助用户轻松构建、管理和部署任意规模的API。专享版API网关按使用版本和出口带宽的实际使用时长收取费用。

API网关服务管理费用详情，请参见产品价格详情。

专享版 API 网关计费说明

专享版API网关分两个维度计费：**版本**、**带宽**，二者同时计入收费。

版本计费方式

版本指您购买API网关专享版实例时，按不同的实例版本收取相应的费用，实例版本分为基础版、专业版、企业版、铂金版，不同版本收费价格不一。

- 按需付费（小时）：这种购买方式比较灵活，可以即开即停，API网关专享版实例从“开通”开启计费到“关闭（欠费）”或“删除”结束计费，以秒为单位统计时长，按实际使用时长计费。

带宽计费方式

带宽指您的API后端服务部署在公网时，另外收取的API请求出公网带宽费用。出公网带宽费用按**带宽大小**以及**使用时长**计费。

说明

- 专享版实例部署在虚拟私有云中，如果您的后端服务也部署在相同虚拟私有云，可直接通过私有地址访问，无需购买带宽。
- 专享版实例的API如从公网调用，实例需绑定一个弹性公网IP，作为公网入口。弹性公网IP需要单独购买。
- 专享版实例的API如仅在VPC内调用，无需购买/绑定弹性公网IP。

2 快速入门

2.1 概述

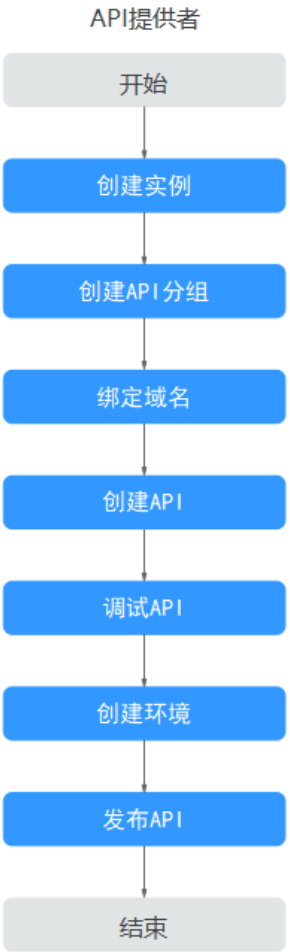
API网关（API Gateway）是为您提供高性能、高可用、高安全的API托管服务，帮助您轻松构建、管理和部署任意规模的API。借助API网关可以简单、快速、低成本、低风险地实现内部系统集成、业务能力开放。

若您想快速体验开放API和调用API的操作流程，请参考**开放API**和**调用API**。这里以APP认证类型的**简易认证**举例，端到端操作快速上手。

2.2 开放 API

2.2.1 开放 API 流程

作为API提供者开放API，您需要先后完成以下流程：



1. 创建实例。
   使用API网关专享版，需要**购买实例**。
2. **创建API分组**
   API分组相当于API的集合，您在创建API前，需要先创建API分组。
3. **绑定域名**
   开放API前，您需要为API分组绑定独立域名（即自定义域名），API调用者通过访问独立域名来调用您开放的API。
4. **创建API**
   创建API包括定义API前后端的请求路径、参数、请求相关协议等。
5. **调试API**
   提供调试功能，调试API接口，验证服务是否正常。
6. **创建环境（可选）**
   API可以同时提供给不同的场景调用，如生产环境（RELEASE）及其他自定义环境。RELEASE是默认存在的环境，无需创建。
7. **发布API**
   只有在将API发布到环境后，API才支持被调用。

2.2.2 创建 API 分组

步骤1 登录API网关控制台。

步骤2 在左侧选择已购买实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击“创建API分组 > 直接创建”。

图 2-1 配置分组信息

表 2-1 配置分组信息

参数	配置说明
分组名称	填写API分组名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
描述	对分组的介绍。

步骤5 单击“确定”，创建API分组。系统会同时为其分配一个调试域名，您可以用于调试API。

----结束

2.2.3 绑定域名

步骤1 在“API分组”页面，单击创建API分组中分组名称，进入分组详情页面。

步骤2 单击“分组信息”页签。

步骤3 在“域名管理”区域，单击“绑定独立域名”，填写要绑定的域名。

图 2-2 绑定独立域名

说明

填写的独立域名已备案，并且已解析，详情请参考**绑定域名**章节的“前提条件”。

----结束

2.2.4 创建 API

创建API步骤：

1. **前端配置**
2. **后端配置**

前端配置

步骤1 在左侧导航栏选择“API管理 > API列表”。

步骤2 单击“创建API”，配置前端定义。

表 2-2 前端定义

参数	配置说明
API名称	填写API名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
所属分组	默认**创建API分组**中已创建分组。
URL	请求方法：接口调用方式，此处选择“POST”。 请求协议：选择协议类型，此处选择“HTTPS”。 子域名：**创建API分组**时，系统默认分配的一个子域名。 路径：接口请求的路径。
网关响应	API网关未能成功处理API请求，从而产生的错误响应。 默认的网关响应为“default”。
匹配模式	默认“绝对匹配”。
标签	标签主要用于对API添加分类属性，方便在创建了大量API后，快速过滤和查找。
描述	API的描述。

步骤3 根据下表参数信息，配置安全配置。

表 2-3 定义 API 请求

参数	配置说明
安全认证	选择API认证方式，此处选择“APP认证”。
支持简易认证	简易认证不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。此处勾选简易认证。

步骤4 单击“下一步”。

----结束

后端配置

步骤1 在“后端配置”页面，配置后端服务信息。

步骤2 选择后端服务类型，此处选择“HTTP/HTTPS”。

表 2-4 HTTP/HTTPS 类型定义后端服务

服务参数	参数说明
负载通道	选择“不使用”负载通道访问后端服务。
URL	请求方法：接口调用方式，此处选择“POST”。 请求协议：选择协议类型，此处选择“HTTP”。 后端服务地址：后端服务的地址。 路径：后端服务的路径。
后端超时	后端服务请求的超时时间。此处默认“5000”ms。

步骤3 在“返回结果基础定义”页面，定义返回结果。

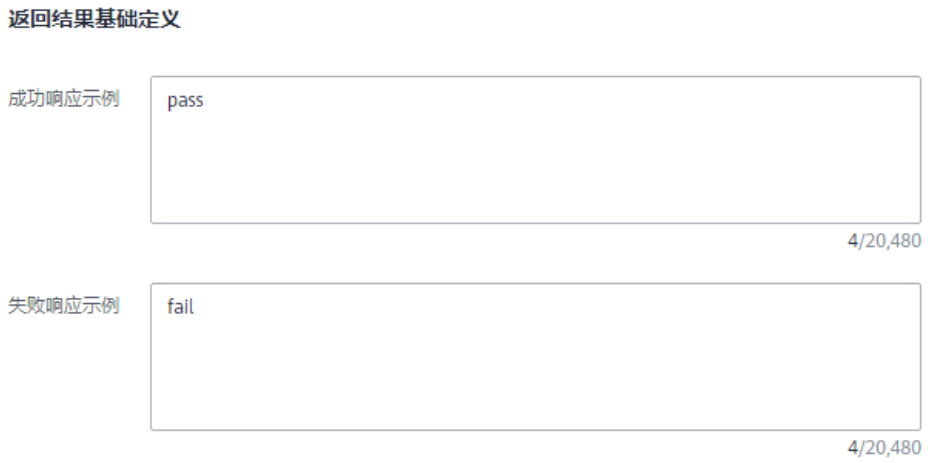


表 2-5 定义返回结果

信息项	描述
成功响应示例	成功调用API时，返回的响应信息示例。
失败响应示例	调用API失败时，返回的响应信息示例。

步骤4 单击“完成”，完成API的创建。

----结束

2.2.5 调试 API

步骤1 在“API运行”页面的左侧选择**已创建API**，单击“调试”。

步骤2 配置API请求参数，此处不配置。

步骤3 单击“调试”，下方为API发送的请求信息和API请求调用后的返回结果回显。

若调用成功时，状态码显示“200”。

----结束

2.2.6 创建环境（可选）

步骤1 在左侧导航栏选择“API管理 > API策略”，单击“环境管理”页签。

步骤2 单击“创建环境”，填写环境信息。

表 2-6 环境信息

参数	配置说明
环境名称	填写API环境名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
描述	环境描述信息。

步骤3 单击“确定”，创建环境。

----结束

2.2.7 发布 API

步骤1 在左侧导航栏选择“API管理 > API列表”。

步骤2 在已**创建API**所在行，单击“发布”。

步骤3 选择API需要发布到的环境。

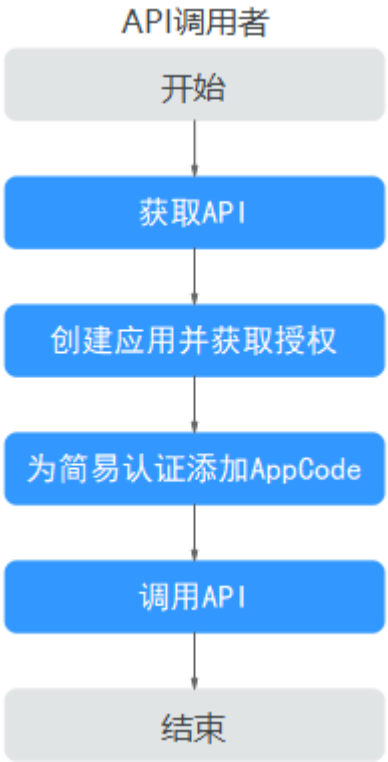
步骤4 单击“确定”。

----结束

2.3 调用 API

2.3.1 调用 API 流程

作为API调用者调用API，您需要完成以下流程：



1. 获取API
   从API提供者中获取API和文档信息。
2. **创建凭据并获取授权**
   使用APP认证的API，需要在API网关中创建一个凭据，并且绑定API后，才可以使用APP认证调用API。
3. **为简易认证添加AppCode**
   使用简易认证，API网关也仅校验AppCode。
4. **调用API**
   为简单起见，此处使用接口测试工具，通过APP认证方式中的凭证来实现对API的调用。

2.3.2 创建凭据并获取授权

创建凭据

步骤1 在左侧导航栏选择“API管理 > 凭据管理”。

步骤2 单击“创建凭据”，填写凭据信息。

表 2-7 凭据信息

信息项	描述
凭据名称	填写凭据名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
描述	对凭据的介绍。

步骤3 单击“确定”。

----结束

绑定 API

步骤1 在“关联API”区域，单击“绑定API”。

步骤2 选择**开放API**中的运行环境、API分组和API，单击“确定”，完成API绑定策略。

----结束

2.3.3 为简易认证添加 AppCode

步骤1 在凭据列表中单击已**创建凭据**名称，进入凭据详情。

步骤2 在“AppCodes”区域。

步骤3 单击“添加AppCode”。

步骤4 在弹窗中选择“自动生成”生成方式。

步骤5 单击“确定”。

----结束

2.3.4 调用 API

使用接口测试工具配置调用信息。

步骤1 获取API请求信息。

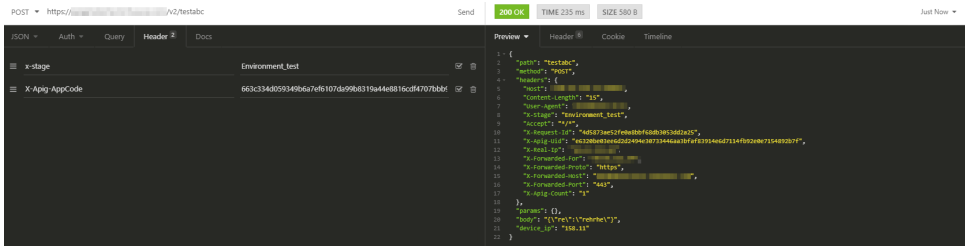
为简单起见，此处通过线下传递方式获取API及文档。API调用者可以从中获取API认证方式，请求方法，请求路径等信息。

步骤2 增加Header参数名称：X-Apig-AppCode，参数值填**已生成的AppCode**。

步骤3 增加Header参数名称：x-stage，参数值为**运行环境**。若API发布到RELEASE环境不需执行此步骤。

步骤4 单击“Send”发送请求。

调用成功后，显示“200 OK”。



----结束

3 新旧版本差异

自2023年4月2日起，API网关界面更新，新旧版本差异点如下表所示。

表 3-1 新旧版差异

差异点	旧版	新版
API的安全配置支持双重认证	无	有
HTTP&HTTPS后端服务类型支持定义重试次数	无	有
导入API	导入API	创建API分组时，支持导入Swagger文件；API列表页支持导入API
API调试可自定义body体	无	有
API详情页布局	API详情页信息集成度一般	API运行页信息集成度高
API详情页：单击流程图切换信息	有	无
可视化查看API已绑定的所有策略	无	有
策略创建和编辑可切换脚本模式	无	有
插件类型	跨域资源共享、HTTP响应头管理、流量控制	跨域资源共享、HTTP响应头管理、流量控制2.0、Kafka日志推送、断路器，与传统策略（流量控制、访问控制、签名密钥）合并于策略管理
SSL证书管理	无	有
负载通道支持创建服务器分组	无（负载通道即VPC通道）	有

差异点	旧版	新版
负载通道提供健康检查开关	无（负载通道即VPC通道）	有
负载通道展示备用节点和启停状态	无（负载通道即VPC通道）	有
应用管理	应用管理	更名凭据管理
凭据配额策略	无	有
访问控制策略	无	有
监控管理	监控管理	更名API监控
子域名	子域名	更名调试域名
变量管理	变量管理	更名环境变量
左侧导航栏上方支持快速切换实例下拉框	无	有

4 总览

API网关（API Gateway）是为您提供高性能、高可用、高安全的API托管服务，帮助您轻松构建、管理和部署任意规模的API。借助API网关可以简单、快速、低成本、低风险地实现内部系统集成、业务能力开放及业务能力变现。

使用流程

使用API网关进行API的托管流程如下图所示。

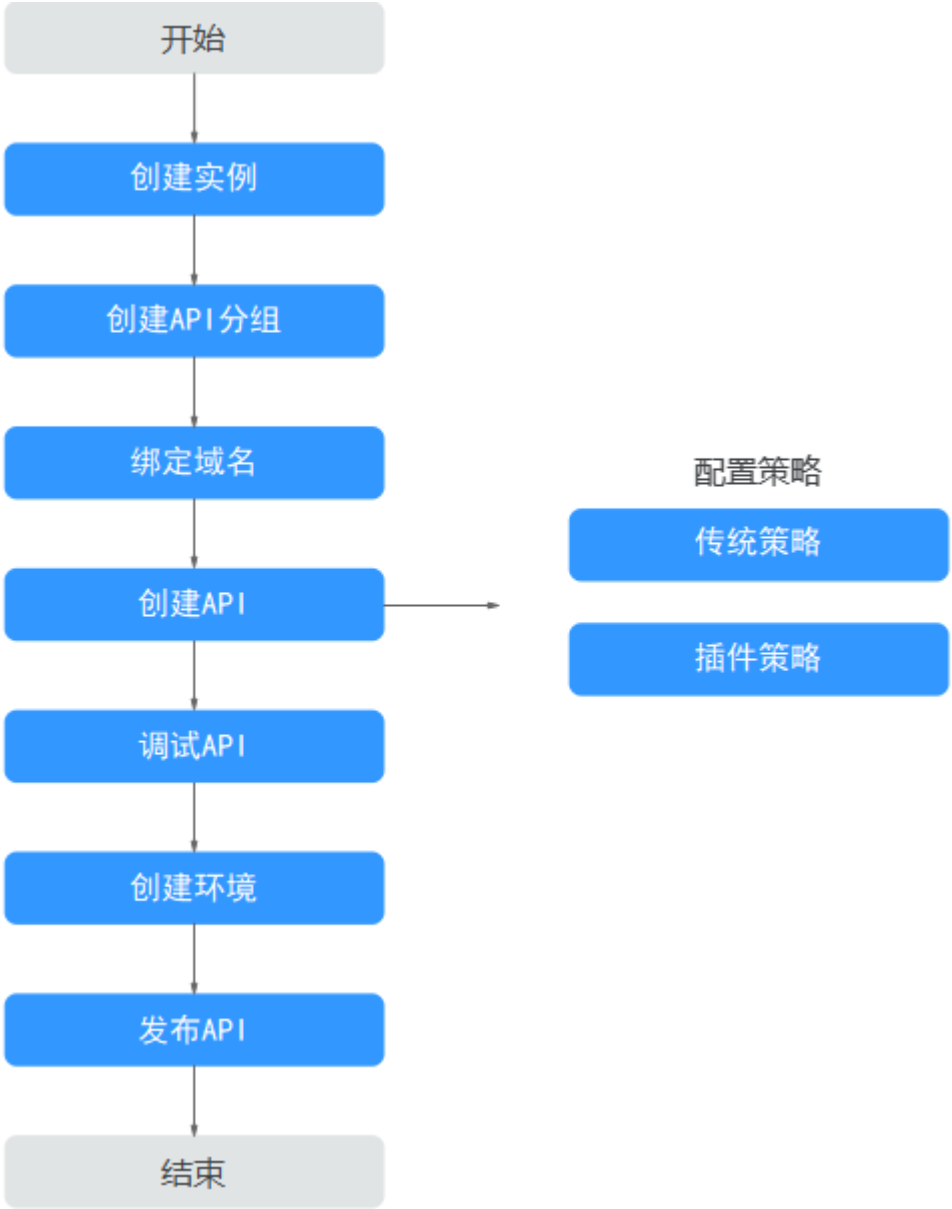
图 4-1 API 网关

API提供者在API网关中**开放自己的API服务**，API调用者从API网关中**获取并调用API**。

开放 API

企业或开发者通过API网关开放自身的服务与数据，实现业务能力变现。

图 4-2 开放 API 基本流程



1. **创建实例**

   实例是一个独立的资源空间，所有的操作都是在实例内进行，不同实例间的资源相互隔离。

2. **创建API分组**

   每个API都归属到某一个API分组下，在创建API前应提前创建API分组。

3. **绑定域名**

   在开放API前，您需要为API分组绑定一个独立域名，供API调用者访问API使用。

   在绑定独立域名前，您可以使用系统为API分配的调试域名进行API调试，每天最多可以访问调试域名1000次。

4. **创建API**

   把已有后端服务封装为标准RESTFul API，并对外开放。

   API创建成功后，您可根据业务需求对API设置访问策略：

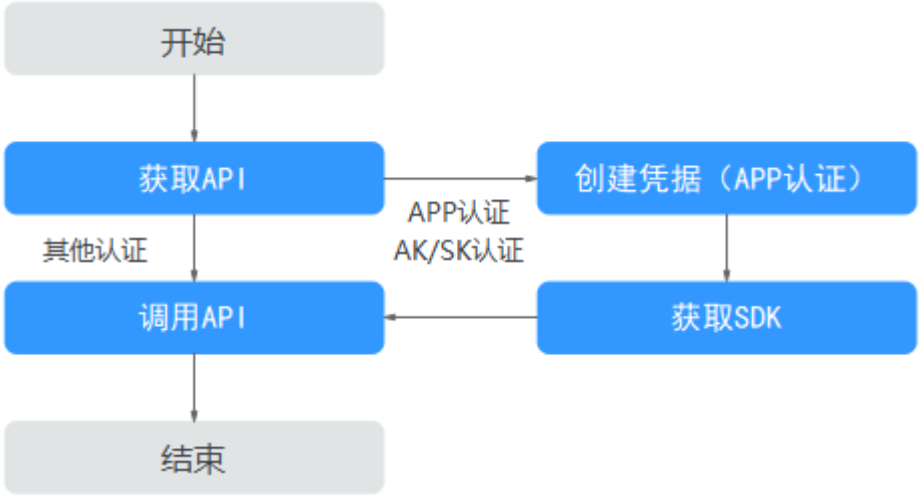
- 传统策略
  - **流控控制**
    流量控制可限制单位时间内API的被调用次数，保护后端服务。
  - **访问控制**
    访问API的IP地址和帐户，您可以通过设置IP地址或帐户的黑白名单来拒绝/允许某个IP地址或帐户访问API。
  - **签名密钥**
    签名密钥用于后端服务验证API网关的身份，在API网关请求后端服务时，保障后端服务的安全。
- 插件策略
  - **跨域资源共享策略说明**
    跨域资源共享策略为跨域访问提供指定预检请求头和响应头、自动创建跨域预检请求API的扩展能力，可快速、灵活的实现API的跨域访问。
  - **HTTP响应头管理策略说明**
    您可以自定义HTTP响应头，在返回的API响应中指定您配置的响应头。
  - **流量控制2.0策略说明**
    您可以限制单位时间内API的被调用次数，支持参数流控、基础流控和基于基础流控的特殊流控。
  - **Kafka日志推送策略说明**
    Kafka日志推送策略提供了把API的详细调用日志推送到Kafka的能力，方便用户获取API的调用日志信息。
  - **断路器策略说明**
    断路器是API网关在后端服务出现性能问题时保护系统的内置机制。

5. **调试API**
   验证API服务的功能是否正常可用。
6. **发布API**
   把API发布到环境中，API只有在发布到环境后，才支持被调用。

调用 API

企业或开发者如何获取并调用他人在API网关开放的API，减少开发时间与成本。

图 4-3 调用 API 基本流程



1. **获取API**

   获取API的请求信息，包括访问域名、请求协议、请求方法、请求路径以及认证方式等信息。

2. **创建凭据**

   使用APP认证的API，需要在API网关中创建一个凭据，以生成凭据ID和密钥对（Key、Secret）。将创建的凭据绑定API后，使用APP认证调用API。

3. **获取SDK**

   可通过SDK对AK/SK生成签名，并调用API。

4. **调用API**

   通过获取API及API访问地址，调用API。根据API使用认证方式的不同，调用API时需要进行不同的认证鉴权操作。

登录 API 网关新版控制台

步骤1 登录控制台。

步骤2 将鼠标移至左侧 ☰ 图标展开服务列表，输入“apig”搜索。

步骤3 单击搜索结果，进入API网关控制台。

使用API网关前，请先创建实例，具体操作请参见**购买实例**章节。

----结束

5 API 管理

5.1 创建 API 分组

创建API前，需要先创建API分组。API分组相当于API的集合，API提供者以API分组为单位，管理分组内的所有API。

目前支持以下创建分组方式：

- 直接创建
  创建一个简单的分组，不包含API，用户可自行创建API。
- 导入API设计文件
  从本地导入已有的API文件，同步创建分组。

说明

- 对外开放API时，您需要为API分组绑定自己的独立域名。
- 一个API只能属于某一个API分组。
- API分组创建后，系统为分组自动分配一个内部测试用的调试域名，此调试域名每天最多可以访问1000次。
- 实例创建后，有一个DEFAULT分组，可直接通过虚拟私有云地址调用默认分组中的API。

前提条件

已创建实例。

直接创建

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击“创建API分组 > 直接创建”，在弹框中填写分组信息。

表 5-1 分组信息表

信息项	描述
分组名称	API分组名称，用于将API接口进行分组管理。
描述	对分组的介绍。

步骤5 单击“确定”，创建完成。

----结束

导入 API 设计文件

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击“创建API分组 > 导入API设计文件”。

步骤5 在弹窗中选择本地路径下的API文件，然后单击“打开”导入文件。

步骤6 填写导入信息。

表 5-2 导入 API

参数名称	说明
导入方式	导入方式包含以下2种： ● 生成新的分组：将API定义导入到一个新的分组，导入过程中系统会自动创建一个新的API分组，并将导入的API归属到该分组。 ● 选择已有分组：将API定义导入到一个已有的分组，导入过程中不会删除分组中已有的API，只是将新增的API导入分组。
API分组	仅在选择“选择已有分组”时，需要选择API分组。
是否覆盖	勾选后，当导入的API名称与已有的API名称相同时，导入的API会覆盖已有的API。 仅在选择“选择已有分组”时，需要选择是否覆盖。
扩展覆盖	勾选后，当导入API扩展定义项名称（ACL，流控等）与已有的策略（ACL，流控等）名称相同时，会覆盖已有的策略（ACL，流控等）。

步骤7 （可选）单击“全局配置(可选)”。

1. 安全配置。请参考5.2。
2. 后端请求配置。请参考步骤1。
3. 单击“下一步”，支持通过“表单”、“JSON”、“YAML”样式查看配置详情。

4. 确认无误后，单击“提交”，完成配置。

步骤8 单击“立即导入”，在弹窗中选择是否现在发布API到环境。

- 如果选择“现在发布”，还需要选择API要发布的环境，将API分组下的所有API发布到环境上。
- 如果选择“稍后发布”，请参考**发布API**。

步骤9 单击“确定”，跳转到“API运行”页面，可查看分组下的API。

----结束

后续操作

API分组创建成功后，您可以为此分组**绑定域名**，API调用者通过访问独立域名来调用您开放的API。

5.2 绑定域名

在开放API前，您需要为API分组绑定独立域名，API调用者通过独立域名访问分组内的API。您也可以使用系统分配的调试域名访问API分组内的API。

- 调试域名（子域名）：API分组创建后，系统为分组自动分配一个内部测试用的调试域名，此调试域名唯一且不可更改，每天最多可以访问1000次。
- 独立域名：您自定义的域名。最多可以添加5个独立域名，不限访问次数。API调用者通过访问独立域名来调用您开放的API。

说明

- 同一实例下的不同分组不能绑定相同的独立域名。
- 调试域名默认只能在与实例相同VPC内的服务器上解析和访问，如果调试域名要支持公网解析与访问，请在实例上绑定公网入口弹性IP。

前提条件

1. 已有独立域名。
2. 已将独立域名A记录解析到实例的入口地址上，具体方法请参见《云解析服务用户指南》的“管理记录集”章节。
3. 如果API分组中的API支持HTTPS请求协议，那么在独立域名中需要添加SSL证书，请您提前获取SSL证书的内容和密钥，并**创建SSL证书**。

操作步骤

步骤1 **登录API网关控制台**。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 单击“分组信息”页签。

步骤6 在“域名管理”区域，单击“绑定独立域名”，并在弹窗中配置域名信息。

表 5-3 独立域名配置

信息项	描述
域名	填写要绑定的域名。
支持最小TLS版本	选择域名访问所使用的最小TLS版本，TLS1.1或TLS1.2，推荐使用TLS1.2。 该配置仅对HTTPS生效，不影响HTTP或者其他访问方式。

步骤7 单击“确定”，将独立域名与API分组绑定。

如果不再需要此域名时，在域名所在行，单击“解绑域名”。

步骤8 （可选）如果API分组中的API支持HTTPS请求协议，则需要为独立域名绑定SSL证书。否则跳过此步骤。

1. 在域名所在行单击“选择SSL证书”。
2. 在选择SSL证书弹窗中勾选要绑定的SSL证书，然后单击“确定”，完成SSL证书的绑定。
   - 如果证书列表中无可用的SSL证书，可单击“创建SSL证书”，新增SSL证书，具体操作配置请参考**创建SSL证书**。

----结束

常见问题

- 绑定域名失败常见原因：未将独立域名CNAME解析到分组的调试域名上或域名重复。
- 添加SSL证书失败常见原因：生成证书的域名和实际添加证书所用的域名不一致。

后续操作

绑定独立域名后，您可以开始**创建API**，将API接口配置在API网关中，开放后端能力。

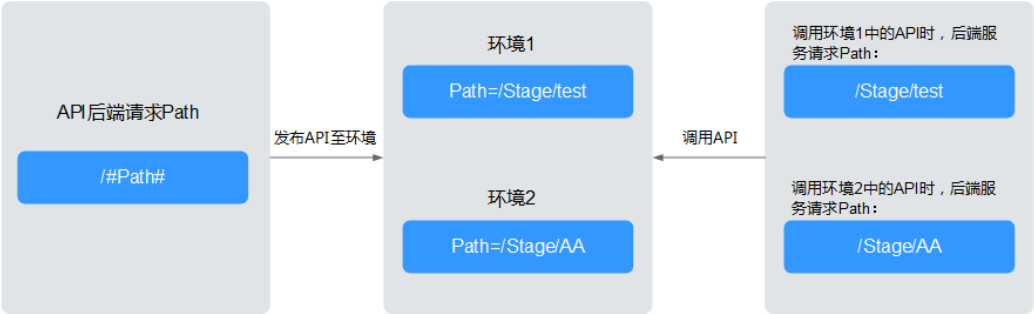
5.3 创建环境变量

API网关提供环境变量功能，通过创建环境变量，实现在不同的环境定义不同的API调用路径。

环境变量是指在环境上创建可管理的一种变量，该变量固定在环境上。通过创建环境变量，实现同一个API，在不同环境中调用不同的后端服务。

当创建API时定义了变量标识，则需要在环境中添加变量。例如创建API时定义了变量名为“Path”，在环境1中创建了变量名“Path”，变量值“/Stage/test”，则API在发布到环境1时，使用“/Stage/test”代替“Path”，API调用者在环境1中调用此API时，后端服务请求Path为“/Stage/test”。在环境2中创建了变量名“Path”，变量值“/Stage/AA”，则API在发布到环境2时，使用“/Stage/AA”代替“Path”，API调用者在环境2中调用此API时，后端服务请求Path为“/Stage/AA”。

图 5-1 环境变量示意图



操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 单击“分组信息”页签。

步骤6 在“环境变量”区域，选择环境。如果未创建环境，可单击“创建环境”创建。

步骤7 单击“添加环境变量”，填写变量信息。

须知

在实际发送API请求中，环境变量名称与变量值会明文传递，请勿携带隐私信息。

表 5-4 新增变量

信息项	描述
变量名	变量的名称，必须与创建API时定义的变量标识完全相同。
变量值	变量路径。

步骤8 单击“确定”，创建完成。

----结束

5.4 新增网关响应

网关响应指API网关未能成功处理API请求，从而产生的错误响应。API网关提供默认的网关响应（default），如果您需要自定义响应状态码或网关响应内容，可在API分组管理中新增网关响应，其中响应内容符合JSON格式即可。

例如，“default”网关的响应内容为：

```
{"error_code": "$context.error.code", "error_msg": "$context.error.message", "request_id": "$context.requestId"}
```

您可以自定义为：

```
{"errorcode": "$context.error.code", "errormsg": "$context.error.message", "requestid": "$context.requestId","apiId":"$context.apiId"}
```

JSON体的内容可以按需定制，包括增减字段内容。

说明

- 每个分组最多可新增4个网关响应。
- 不论是默认网关响应“default”或是您自定义的网关响应，响应类型范围固定不可修改。您可以修改每种响应的状态码，以及响应内容。
- 网关响应所定义的错误类型固定且不可修改，具体见**网关错误响应类型说明**。
- 响应内容支持调用API网关运行时变量（$context变量），具体见**API网关运行时可获取变量**。

操作步骤

步骤1 **登录API网关控制台**。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 单击“分组信息”页签。

步骤6 在“网关响应”区域，您可以新增或编辑网关响应。

如果修改完默认网关响应后，需要恢复默认配置，单击“恢复默认配置”即可。

----结束

网关错误响应类型说明

API网关提供的错误响应类型见下表，其中响应状态码可以按实际需要做自定义修改。

表 5-5 API 网关的错误响应类型

错误说明	默认的响应状态码	详细说明
拒绝访问	403	拒绝访问，如触发配置的访问控制策略、或异常攻击检测拦截
自定义认证配置错误	500	自定义认证方异常，通信失败、返回异常响应等错误
自定义认证失败	500	自定义认证方返回认证失败
自定义认证身份来源错误	401	前端自定义认证的身份来源信息缺失或不合法错误
认证失败	401	认证失败，IAM或APP认证校验失败

错误说明	默认的响应状态码	详细说明
认证身份来源缺失	401	认证身份来源信息缺失
后端超时	504	后端超时，与后端的网络交互超过预配置的时间错误
后端不可用	502	后端不可用，网络不可达错误
默认4XX	-	其它4XX类错误
默认5XX	-	其它5XX类错误
未找到匹配的API	404	未匹配到API
请求参数错误	400	请求参数校验失败、不支持的HTTP方法
调用次数超出阈值	429	API调用次数超出所配置的流量策略阈值
凭据未授权	401	使用的凭据未被授权访问该API

API 网关运行时可获取变量

表 5-6 网关错误响应消息体支持的变量

运行时变量名称	描述
$context.apiId	API的ID
$context.appId	API调用者的凭据对象ID
$context.requestId	当次API调用生成请求ID
$context.stage	API调用的部署环境
$context.sourceIp	API调用者的源地址
$context.authorizer.frontend.property	前端自定义认证响应的context映射的指定键值对的字符串值
$context.authorizer.backend.property	后端自定义认证响应的context映射的指定键值对的字符串值
$context.error.message	当前网关错误响应的错误信息
$context.error.code	当前网关错误响应的错误码
$context.error.type	当前网关错误响应的错误类型

5.5 创建 API

API提供者把API接口配置在API网关中，开放后端能力。创建API分以下步骤：

- **前端配置**
  支持配置前端定义、安全配置和请求参数。
- **后端配置**
  支持配置默认后端、策略后端和返回结果。
- **（可选）为API添加策略**
  支持配置传统策略和插件策略。

说明

API网关服务基于REST的API架构，API的开放和调用需要遵循RESTful相关规范。

前提条件

- 已创建API分组。如果未创建API分组，请**创建API分组**。
- 如果后端服务需要使用负载通道，请**创建负载通道**。
- 如果需要使用自定义认证方式进行API的安全认证，请**创建自定义认证**。

前端配置

步骤1 **登录API网关控制台**。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 在“API运行”页面，单击“创建API”。

1. 根据下表参数信息，配置前端定义。

表 5-7 前端定义

信息项	描述
API名称	API名称，根据规划自定义。建议您按照一定的命名规则填写API名称，方便您快速识别和查找。
所属分组	API所属的分组。
URL	前端地址由请求方法、请求协议、子域名和路径组成。 – 请求方法：GET、POST、DELETE、PUT、PATCH、HEAD、OPTIONS、ANY。其中ANY表示该API支持任意请求方法。 – 请求协议：HTTP、HTTPS、HTTP&HTTPS，传输重要或敏感数据时推荐使用HTTPS。 – 子域名：所在分组的调试域名。 – 路径：接口请求的路径。请求路径可以包含请求参数，请求参数使用{}标识，例如/a/{b}，也可以通过配置“+”号做前缀匹配，例如：/a/{b+}。

信息项	描述
网关响应	网关响应指未能成功处理API请求，从而产生的错误响应。 API网关提供默认的网关响应（default）。如果您需要自定义响应状态码或网关响应内容，可在API分组中**新增网关响应**，按照您自己的响应内容，符合JSON格式即可。
匹配模式	分为两种模式： – 绝对匹配：调用的请求Path固定为创建时填写的API请求Path。 – 前缀匹配：调用的请求Path将以创建时填写的API请求Path为前缀，支持接口定义多个不同Path。例如，请求路径为/test/AA，使用前缀匹配时，通过/test/AA/CC可以访问，但是通过/test/AACC无法访问。 **说明** 使用前缀匹配时，匹配剩余的路径将透传到后端。 例如，使用前缀匹配，前端请求路径定义为/test/，后端请求路径定义为/test2/，通过/test/AA/CC访问API，则后端收到的请求url为/test2/AA/CC。
标签	标签主要用于对API添加分类属性，方便在创建了大量API后，快速过滤和查找。
描述	API的描述。

2. 根据下表参数信息，配置安全配置。

表 5-8 安全配置

信息项	描述
类型	API类型： – 公开。

信息项	描述
安全认证	API认证方式： – APP认证：表示由API网关服务负责接口请求的安全认证。推荐使用APP认证方式。 – IAM认证：表示借助IAM服务进行安全认证。 – 自定义认证：用户有自己的认证系统或服务（如使用OAuth认证），可选择“自定义认证”。 – 无认证：表示不需要认证。 各种认证方式下的API调用稍有不同，具体请参考《API网关开发指南》。 **须知** – 认证方式为IAM认证时，任何API网关租户均可以访问此API，可能存在恶意刷流量，导致过量计费的风险。 – 认证方式为无认证时，任何公网用户均可以访问此API，可能存在恶意刷流量，导致过量计费的风险。 – 认证方式为自定义认证时，需要在函数服务中写一段函数，对接用户自己的认证系统或服务。如果当前Region没有上线函数工作流服务，则不支持自定义认证。
支持简易认证	**仅当“安全认证”选择“APP认证”时可配置。** 简易认证指APP认证方式下调用API时，在HTTP请求头部消息增加一个参数X-Apig-AppCode，而不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。 注意仅支持HTTPS方式调用，不支持HTTP方式。具体使用请参考**为简易认证绑定AppCode**。 **说明** 如果首次创建API未开启简易认证，那么之后开启简易认证，需要重新发布API。请参考**发布API**发布。
支持双重认证	**仅当“安全认证”选择“APP认证”或“IAM认证”时可配置。** 是否对API的调用进行双重安全认证。如果选择启用，则在使用APP认证或IAM认证对API请求进行安全认证时，同时使用自定义的函数API对API请求进行安全认证。
自定义认证	**仅当“安全认证”选择“自定义认证”时需要配置。** 自定义认证需要提前创建，可单击右侧的“新建自定义认证”链接创建。

信息项	描述
支持跨域CORS	是否开启跨域访问CORS（cross-origin resource sharing）。 CORS允许浏览器向跨域服务器，发出XMLHttpRequest请求，从而克服了AJAX只能同源使用的限制。 CORS请求分为两类： – 简单请求：头信息之中，增加一个Origin字段。 – 非简单请求：在正式通信之前，增加一次HTTP查询请求。 开启CORS（非简单请求）时，您需要单独创建一个“请求方法”为“OPTIONS”的API，具体操作请参考开启跨域访问。

3. （可选）根据实际需要定义API的请求参数，请求参数定义见下表。

表 5-9 请求参数

信息项	描述
参数名	参数的名称，如果参数在“Path”位置，参数名称会同步“路径”中的名称。 **说明** – 参数名不能是x-apig- 、x-sdk-开头，不区分大小写。 – 参数名不能是x-stage，不区分大小写。 – 参数位置为HEADER时，参数名不能是“Authorization”和“X-Auth-Token”，不区分大小写，也不支持下划线。
参数类型	字段的类型，包含STRING和NUMBER。 **说明** 入参如果为boolean，请选择STRING。
必填	请求API时，此参数是否为必填。如果选择“是”，API网关将校验请求中是否包含此参数，如果不包含，则拒绝该请求。
透传	请求参数是否透传到后端服务。
枚举	请求参数的枚举值，请求参数的值只能从枚举值中选择，多个枚举值间用英文逗号隔开。
默认值	“必填”为“否”时，默认值生效。请求中不包含此参数时，API网关自动增加默认值发送给后端服务。
字节限制	– 最大长度/最大值：“类型”为“STRING”时，设置参数值的最大字符串长度，“类型”为“NUMBER”时，设置参数值的最大值。 – 最小长度/最小值：“类型”为“STRING”时，设置参数值的最小字符串长度，“类型”为“NUMBER”时，设置参数值的最小值。

信息项	描述
示例	参数值的填写示例。
描述	对于此参数的描述。

步骤6 单击“下一步”，进入后端配置。

----结束

后端配置

支持定义多个策略后端，即满足一定条件后转发给指定的API后端服务，用以满足不同的调用场景。例如为了区分普通调用与特殊调用，可以定义一个“策略后端”，通过调用方的源IP地址，为特殊调用方分配专用的后端服务。

除了定义一个默认的API后端服务，一个API共可以定义5个策略后端。

步骤1 定义默认后端。

添加策略后端前必须定义一个默认后端，当不满足任何一个策略后端的API请求，都将转发到默认的API后端。

在“后端配置”页面，选择API后端服务类型。

后端服务类型分HTTP&HTTPS、FunctionGraph和Mock三种，具体参数描述见表5-10、表5-11、表5-12。

说明

- FunctionGraph依赖于函数工作流服务FunctionGraph，如果当前环境中未部署FunctionGraph服务，则后端服务类型FunctionGraph不可用。
- 在后端服务还不具备的场景下，可以使用Mock模式，将预期结果固定返回给API调用方，方便调用方进行调试验证。

表 5-10 HTTP&HTTPS 类型定义后端服务

信息项	描述
负载通道	是否使用负载通道访问后端服务。如果选择“使用”，您需要提前创建负载通道。

信息项	描述
URL	URL地址由请求方法、请求协议、负载通道/后端服务地址和路径组成。 ● 请求方法 GET、POST、DELETE、PUT、PATCH、HEAD、OPTIONS、ANY，其中ANY表示该API支持任意请求方法。 ● 请求协议 HTTP或HTTPS，传输重要或敏感数据时推荐使用HTTPS。 **说明** – 支持WebSocket通信。 – 定义的后端服务协议须与用户的后端业务协议保持一致。 ● 负载通道（可选） **仅在使用负载通道时，需要设置**。选择已创建的负载通道名称。 **说明** 负载通道中，云服务器的安全组必须允许100.125.0.0/16网段访问，否则将导致健康检查失败及业务不通。 ● 后端服务地址（可选） **仅在不使用负载通道时，需要设置**。 填写后端服务的访问地址，格式：“主机:端口”。主机为后端服务的访问IP地址/域名，未指定端口时，HTTP协议默认使用80端口，HTTPS协议默认使用443端口。 如果后端服务地址中需要携带环境变量，则使用“#变量名#”的形式将环境变量添加到后端服务地址中，如#ipaddress#。支持添加多个环境变量，如#ipaddress##test#。 ● 路径 后端服务的路径，即服务的uri，可以包含路径参数，以{路径参数}形式表示，比如/getUserInfo/{userId}。 如果请求路径中含有环境变量，则使用#变量名#的方式将环境变量定义到请求路径中，如/#path#。支持创建多个环境变量，如/#path##request#。
自定义host头域	**仅在使用负载通道时，可设置**。 在请求被发送到负载通道中主机前，允许您自定义请求的host头域，默认将使用请求中原始的host头域。
后端超时(ms)	后端服务请求的超时时间。 如果在API调试过程中，遇到后端响应超时之类的错误，请适当调大后端超时时间，以便排查原因。 **说明** 在实例**配置参数**中修改超时时间上限，可修改范围为1ms~600000ms。

信息项	描述
重试次数	后端服务请求失败后的重试次数，默认值为-1，取值范围-1~10。 ● 值为-1时，表示不开启重试功能，但除POST和PATCH外的其他请求类型会默认重试1次。 ● 值为0-10时，表示开启重试功能，并根据设置的值执行重试。当值为0时，不重试。 **使用负载通道时**，重试次数应小于负载通道中已启用的后端服务器个数。
TLS双向认证	**仅在协议为“HTTPS”时，可设置。** 选择是否在API网关和后端服务间启用双向认证，如果选择“使用backend_client_certificate配置的证书做客户端认证”，您需在实例的“配置参数”中提前配backend_client_certificate证书。
后端认证	当您的后端服务需要对API调用增加自己的认证，则开启后端认证。 后端认证需要先添加一个自定义认证，自定义认证通过函数服务实现，在函数服务中编写一个函数，实现您的认证鉴权流程，或者使用函数调用您的统一鉴权服务。 **说明** 后端认证依赖函数服务，此功能仅在部分区域开放。

表 5-11 FunctionGraph 类型定义后端服务

信息项	描述
函数名	添加函数后，函数名自动生成。
函数URN	函数请求唯一标识。 单击“添加”，添加所需的函数URN。
版本或别名	支持选择函数的版本或别名，函数的版本或别名功能请参考《函数工作流 FunctionGraph用户指南》的“版本管理”和“别名管理”章节。
调用类型	● Synchronous：同步调用。指后端函数服务收到调用请求后立即执行并返回调用结果，客户端发送请求后同步等待，收到后端响应后关闭连接。 ● Asynchronous：异步调用。客户端不关注请求调用的结果，服务端收到请求后将请求排队，排队成功后请求就返回，服务端在空闲的情况下会逐个处理排队的请求。
后端超时(ms)	参考表5-10后端超时。
后端认证	参考表5-10后端认证。

表 5-12 Mock 类型定义后端服务

信息项	描述
Mock自定义返回码	选择API响应的HTTP状态码。
Mock返回结果	Mock一般用于开发调试验证。在项目初始阶段，后端服务没有搭建好API联调环境，可以使用Mock模式，将预期结果固定返回给API调用方，方便调用方进行项目开发。
后端认证	参考**表5-10**后端认证。
添加header参数	自定义API响应的header参数。 单击“添加header参数”，并填写参数名、参数值和参数描述。

说明

- 在URL中配置了变量标识后，在API调试页面将无法调试。
- 如果在URL中设置变量，那么必须在待发布环境上配置变量名和变量值，否则变量无法赋值，API将无法正常调用。
- 变量名严格区分大小写。

步骤2 （可选）配置默认后端的后端服务参数，将调用API时传入的请求参数映射到后端服务请求的对应位置。如果**5.3**中未定义请求参数，可直接跳过此步骤。

1. 在“后端服务参数”下，可通过以下任意一种方法添加后端服务参数。
   - 单击“导入入参定义”，把所有已定义的API请求参数添加到后端服务参数。
   - 单击“添加后端参数映射”，按需逐个添加后端服务参数。
2. 根据后端服务实际的参数名称和参数位置修改映射关系，如**图5-2**所示。

图 5-2 配置后端服务参数

a. 后端参数在“PATH”位置，那么参数名称需要和“路径”中的名称相同。
b. 调用API的请求参数名称、位置可以与后端参数名称、位置不同。

   说明

   - 参数名不能是x-apig- 、x-sdk-开头，不区分大小写。
   - 参数名不能是x-stage，不区分大小写。
   - 参数位置为HEADER时，参数名不区分大小写，也不支持下划线开头。

c. 如上图，test01和test03在调用API时分别配置于PATH和QUERY位置，后端服务通过映射，将在HEADER位置接收test01和test03的值。test02在调用API

时配置于HEADER位置，后端服务通过映射，将在PATH位置以参数名test05来接收test02的值。

假设test01为aaa，test02为bbb，test03为ccc。

API调用请求：

```
curl -ik -H 'test02:bbb' -X GET https://example.com/v1.0/aaa?test03=ccc
```

后端服务请求：

```
curl -ik -H 'test01:aaa' -H 'test03:ccc' -X GET https://example.com/v1.0/bbb
```

步骤3 （可选）配置默认后端的常量参数。如果后端服务需要接收固定的常量信息，可以通过设置常量参数来实现。API网关向后端服务发送请求时，将常量参数添加到请求的指定位置，然后将请求发送给后端服务。

在“常量参数”下，单击“添加常量参数”，添加后端服务请求的常量参数。

须知

常量参数会明文展示，为防止信息泄露，请谨慎配置。

表 5-13 常量参数配置

信息项	描述
常量参数名	填写常量参数的名称。“参数位置”为“PATH”时，参数名需要与“路径”中的参数名称一致。 **说明** ● 参数名不能以x-apig- 、x-sdk-开头，不能是x-stage，不区分大小写。 ● 参数位置为HEADER时，参数名不支持下划线开头，不区分大小写。
参数位置	选择常量参数在后端服务请求中的位置，可选择“PATH”、“HEADER”和“QUERY”。
参数值	填写常量参数的值。
描述	填写常量参数的描述信息。

说明

- API网关将包含常量参数的请求发送给后端服务前，会对特殊参数值进行百分号编码，请确保后端服务支持百分号编码。例如，参数值[api]，在百分号编码后变为%5Bapi%5D。
- 对于PATH位置的参数值，API网关会对如下字符进行百分号编码：ASCII码为0到31的字符、?、>、<、/、%、#、"、[、\、]、^、`、{、|、}、空白符、ASCII码为127到255的字符。
- 对于QUERY位置的参数值，API网关会对如下字符进行百分号编码：ASCII码为0到31的字符、>、=、<、+、&、%、#、"、[、\、]、^、`、{、|、}、空白符、ASCII码为127到255的字符。

步骤4 （可选）配置默认后端的系统参数。如果后端服务需要接收系统运行时产生的参数信息，如网关内置参数、前端认证参数和后端认证参数等，可以通过设置系统参数来实

现。API网关向后端服务发送请求时，将系统参数添加到请求的指定位置，然后将请求发送给后端服务。

1. 在“系统参数”下，单击“添加系统参数”，添加后端服务请求的系统参数。

表 5-14 系统参数配置

信息项	描述
系统参数类型	选择系统参数的类型。 – 网关内置参数：支持配置的参数。 – 前端认证参数：前端自定义认证返回结果中的参数。在前端配置中，“安全认证”选择“自定义认证”时，才可以选择此参数。 – 后端认证参数：后端自定义认证返回结果中的参数。在后端配置中，“后端认证”开启时，才可以选择此参数。
系统参数名	填写系统参数的名称。 – “系统参数类型”为“网关内置参数”时，支持选择如下参数： ▪ sourceIp：API调用者的源地址。 ▪ stage：API调用的部署环境。 ▪ apiId：API的ID。 ▪ appId：API调用者的APP ID。 ▪ requestId：当次调用API所生成的请求ID。 ▪ serverAddr：网关服务器的地址 。 ▪ serverName：网关服务器的名称。 ▪ handleTime：本次调用API的处理时间。 ▪ providerAppId：API提供者的凭据ID。 ▪ apiName：API的名称，需要发布API后才可使用此参数。 ▪ appName：调用API所使用的凭据名称。 – 系统参数类型为“前端认证参数”或“后端认证参数”时，支持自定义参数，但是此参数必须为自定义认证返回结果中的参数。 自定义认证函数的编写以及返回结果参数的获取方法，请参考《API网关开发指南》。

信息项	描述
后端参数名称	填写系统参数需要映射的后端参数名称。 **说明** – 参数名不能以x-apig- 、x-sdk-开头，不能是x-stage，不区分大小写。 – 参数位置为HEADER时，参数名不支持下划线开头，不区分大小写。
后端参数位置	选择后端参数在后端服务请求中的位置，可选择“PATH”、“HEADER”和“QUERY”。
描述	填写系统参数的描述信息。

步骤5 （可选）添加策略后端。

添加多个后端策略后，通过不同的策略条件，请求被转发到不同的后端服务中。

1. 单击⊕添加策略后端。
2. 后端策略增加的参数，具体如表5-15所示，其他参数说明参考表5-10、表5-11和表5-12。

表 5-15 后端策略参数

信息项	描述
后端策略名称	您自定义的名称，用于识别不同的后端策略。
生效方式	– 满足任一条件：只要满足策略条件中的任意一项，此后端策略就可以生效。 – 满足全部条件：只有满足所有的策略条件，此后端策略才生效。
策略条件	使后端策略生效的条件，具体如表5-16所示。

表 5-16 策略条件

信息项	描述
条件来源	– 源地址：以访问API的请求地址作为策略条件来源。 – 请求入参：以请求入参参数作为策略条件来源。 – Cookie：表示以API请求的Cookie信息作为判断条件。 – 系统参数：以系统参数作为策略条件来源。系统参数指API网关处理API请求时的系统运行时参数信息。 **须知** – 选择“请求入参”作为策略条件时，入参需要在API前端请求中配置好，如在Header中添加一个参数。 – 如果未展示“系统参数”请联系技术支持升级实例。
参数名称	– 当“条件来源”为“请求入参”时，需要设置。选择已创建的入参参数名称。 – 当“条件来源”为“系统参数”时，需要选择参数名称。 ▪ reqPath：请求URI，如“/a/b/c”。 ▪ reqMethod：请求方法，如“GET”。 – 当“条件来源”为“COOKIE”时，需要填写Cookie中的参数名称。
参数位置	仅在“条件来源”为“请求入参”时，展示请求入参的参数位置。
条件类型	仅在“条件来源”为“请求入参”、“系统参数”、“COOKIE”时需要配置。 – 相等：请求参数值必须为输入值时，条件成立。 – 枚举：请求参数值只需要和枚举值中任何一个值相同，条件成立。 – 匹配：请求参数值只需要和正则表达式中任何一个值相同，条件成立。 **说明** 当“条件来源”为“系统参数”并且“参数名称”为“reqMethod”时，“条件类型”仅支持选择相等或枚举。
条件值	– “条件类型”为“相等”时，输入一个值。 – “条件类型”为“枚举”时，输入多个值，以英文逗号隔开。 – “条件类型”为“匹配”时，输入一个范围，例如：[0-5]。 – “条件来源”为“源地址”时，输入一个或多个IP地址，以英文逗号隔开。

步骤6 定义返回结果。

在“返回结果基础定义”区域，填写返回信息。

表 5-17 定义返回结果

信息项	描述
成功响应示例	成功调用API时，返回的响应信息示例。
失败响应示例	调用API失败时，返回的响应信息示例。

步骤7 单击“完成”，进入“API运行”页面，可查看API详情。

----结束

（可选）为 API 添加策略

发布API后，方可添加策略。

步骤1 在“API运行”页面，单击“添加策略”。

步骤2 选择策略类型，配置策略。

- 选择已有策略：单击“选择已有策略”后，选择策略。
- 创建新策略：请参考**创建策略**。

步骤3 单击“确定”，完成策略的创建。

----结束

创建 API 相关的 FAQ

API网关是否支持多后端节点方案?

如何选择认证方式?

为什么后端服务调用失败?

在API网关中创建完成API，调用时报“No backend available”错误，怎么解决?

后续操作

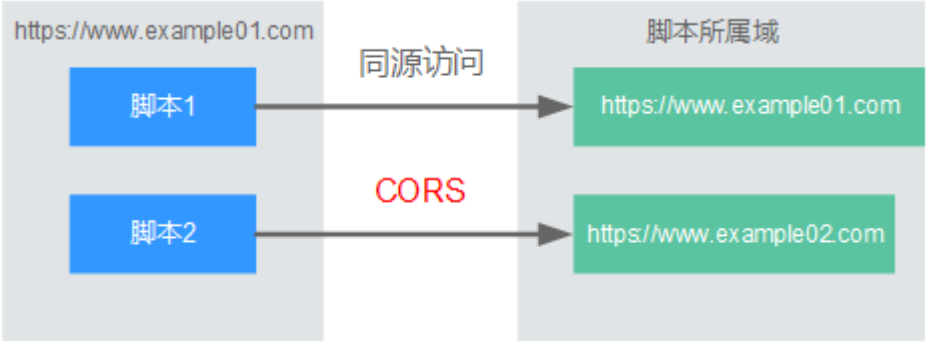
API创建完成后，通过**调试API**，验证服务是否正常。

5.6 开启跨域访问

什么是跨域访问

浏览器出于安全性考虑，会限制从页面脚本内发起的跨域访问（CORS）请求，此时页面只能访问同源的资源，而CORS允许浏览器向跨域服务器，发送XMLHttpRequest请求，从而实现跨域访问。

图 5-3 跨域访问



浏览器将CORS请求分为两类：

- **简单请求**

  简单跨域请求的场景需要满足以下两个条件：

  a. 请求方法是HEAD，GET，或者POST。

  b. HTTP的头信息不超出以下范围：

     - Accept
     - Accept-Language
     - Content-Language
     - Last-Event-ID
     - Content-Type：取值范围：application/x-www-form-urlencoded、multipart/form-data、text/plain

  对于简单请求，浏览器自动在头信息之中，添加一个Origin字段，Origin字段用于说明本次请求来自哪个源（协议+域名+端口）。服务器根据这个值，决定是否同意这次请求。服务器响应消息中包含“Access-Control-Allow-Origin”时，表示同意请求。

- **非简单请求**

  不满足简单请求两个条件的都为非简单请求。

  对于非简单请求，在正式通信之前，浏览器会增加一次HTTP查询请求，称为预检请求。浏览器询问服务器，当前页面所在的源是否在服务器的许可名单之中，以及可以使用哪些HTTP请求方法和头信息字段。预检通过后，浏览器向服务器发送简单请求。

开启跨域访问

API网关默认不开启跨域访问，如果您需要开启，请参考以下说明完成跨域配置。如需自定义跨域的请求头、跨域的请求方法和指定授权访问的域，请使用跨域资源共享策略说明。

- **简单请求的跨域访问**

  如果是创建新的API，在“安全配置”时，打开“支持跨域（CORS）”开关。详细的使用指导，可参考简单请求。

- **非简单请求的跨域访问**

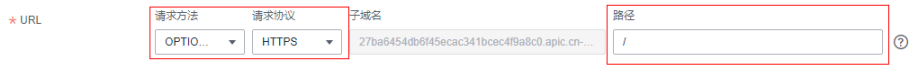
须知

非简单请求的跨域访问需要在API的分组中**创建一个“请求方法”为“OPTIONS”的API，作为预检请求**。

预检请求API的参数设置，请参考以下说明填写。详细的使用指导可参考**非简单请求**。

a. 在“前端定义”中，参数填写说明如下：
   - 请求方法：选择“OPTIONS”
   - 请求协议：选择与已开启CORS的API相同的请求协议
   - 路径：填斜杠/

图 5-4 预检请求-定义 API 请求

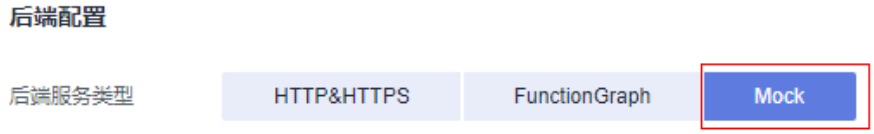


b. 在“安全配置”中，安全认证选“无认证”，勾选“开启支持跨域CORS”。

图 5-5 预检请求-使用无认证方式

c. 后端配置选择“Mock”。

图 5-6 预检请求-后端选 Mock



简单请求

对于简单请求，您需要开启简单跨域访问。

场景一：已开启CORS，且后端服务响应消息中未指定跨域头时，API网关接受任意域的请求，并返回“Access-Control-Allow-Origin”跨域头，示例如下：

浏览器发送一个带Origin字段的请求消息：

```
GET /simple HTTP/1.1
Host: www.test.com
Origin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Origin：此字段必选，表示请求消息所属源，上例中请求来源于“http://www.cors.com”，API网关/后端服务根据这个值，决定是否同意本次请求。

后端服务返回响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway

{"status":"200"}
```

API网关响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: *

{"status":"200"}
```

Access-Control-Allow-Origin：此字段必选，“*”表示API网关接受任意域的请求。

场景二：已开启CORS，且后端服务响应消息中指定跨域头时，后端服务响应的跨域头将覆盖API网关增加的跨域头，示例如下：

浏览器发送一个带Origin字段的请求消息：

```
GET /simple HTTP/1.1
Host: www.test.com
Origin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Origin：此字段必选，表示请求消息所属源，上例中请求来源于“http://www.cors.com”，API网关/后端服务根据这个值，决定是否同意本次请求。

后端服务返回响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
Access-Control-Allow-Origin: http://www.cors.com

{"status":"200"}
```

Access-Control-Allow-Origin：表示后端服务接受“http://www.cors.com”的请求。

API网关响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: http://www.cors.com

{"status":"200"}
```

后端服务响应消息中的跨域头覆盖API网关响应消息中的跨域头。

非简单请求

对于非简单请求，您需要开启跨域访问，并且创建一个“请求方法”为“OPTIONS”的API。

说明

跨域共享资源策略不需要创建一个“请求方法”为“OPTIONS”的API。

“请求方法”为“OPTIONS”的API和普通API的区别如下：

- 所属分组：选择已开启CORS的API所在的分组。
- 请求方法：选择“OPTIONS”。
- 请求协议：选择与已开启CORS的API相同的请求协议。
- 路径：填斜杠/即可，也可选择与已开启CORS的API相同或者匹配的请求Path。
- 安全认证：可选择“无认证”。无论选择哪种认证方式，API网关都按照无认证处理。
- 支持跨域CORS：选择开启CORS。

假设后端服务类型为Mock，示例如下：

浏览器发送“请求方法”为“OPTIONS”的API请求：

```
OPTIONS /HTTP/1.1
User-Agent: curl/7.29.0
Host: localhost
Accept: */*
Origin: http://www.cors.com
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: X-Sdk-Date
```

- Origin：此字段必选，表示请求消息所属源。
- Access-Control-Request-Method：此字段必选，表示请求会使用哪些HTTP请求方法。

- Access-Control-Request-Headers：此字段可选，表示请求会额外发送的头信息字段。

后端服务返回消息：无

API网关返回消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 02:38:48 GMT
Content-Type: application/json
Content-Length: 1036
Server: api-gateway
X-Request-Id: c9b8926888c356d6a9581c5c10bb4d11
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Stage,X-Sdk-Date,X-Sdk-Nonce,X-Proxy-Signed-Headers,X-Sdk-Content-Sha256,X-Forwarded-For,Authorization,Content-Type,Accept,Accept-Ranges,Cache-Control,Range
Access-Control-Expose-Headers: X-Request-Id,X-Apig-Latency,X-Apig-Upstream-Latency,X-Apig-RateLimit-Api,X-Apig-RateLimit-User,X-Apig-RateLimit-App,X-Apig-RateLimit-Ip,X-Apig-RateLimit-Api-Allenv
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,HEAD,OPTIONS,PATCH
Access-Control-Max-Age: 172800
```

- Access-Control-Allow-Origin：此字段必选，“*”表示API网关接受任意域的请求。
- Access-Control-Allow-Headers：当请求消息中包含此字段时，此字段必选。表示允许跨域的所有请求头信息字段。
- Access-Control-Expose-Headers：表示跨域访问允许查看的返回头信息字段。
- Access-Control-Allow-Methods：此字段必选，表示API网关支持的所有HTTP请求方法。
- Access-Control-Max-Age：此字段可选，表示本次预检的有效期，单位：秒。在有效期内，无需再次发出预检请求。

浏览器发送一个带Origin字段的请求头：

```
PUT /simple HTTP/1.1
Host: www.test.com
Origin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

后端服务返回消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway

{"status":"200"}
```

API网关返回消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: *

{"status":"200"}
```

5.7 调试 API

API创建后需要验证服务是否正常，管理控制台提供调试功能，您可以添加HTTP头部参数与body体参数，调试API接口。

说明

- 后端路径中含有环境变量的API，不支持调试。
- 如果API已绑定流控策略，在调试API时，流控策略无效。

前提条件

已搭建完成后端服务。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 在“API运行”页签，选择待调试的API，单击“调试”。

步骤6 配置API请求参数后，单击“调试”。

步骤7 在页面下方返回结果回显区域打印API调用的Response信息。

- 调用成功时，返回HTTP状态码为“200”和Response信息。
- 调试失败时，返回HTTP状态码为4*xx*或5*xx*，具体错误信息请参见错误码。

步骤8 您可以通过调整请求参数与参数值，发送不同的请求，验证API服务。

----结束

后续操作

API调试成功后，您可以将API发布到环境，以便API调用者调用。或者出于API的安全性考虑，为API添加策略。

5.8 授权 API

API在创建后，通过指定授权给某些凭据，让指定凭据能够调用API。

须知

- 仅在API为APP认证时，才支持授权给凭据。
- 单个凭据最多同时授权1000个API。

前提条件

- API已发布。
- 已创建环境。
- 已创建凭据。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 在“API运行”页面，选择待授权的API，单击“更多 > 授权”。

步骤6 单击“添加授权”。

步骤7 选择API授权环境，查询并勾选凭据后，单击“确定”。在“授权历史”弹窗中展示已授权的凭据。

如果已授权的凭据需要解除授权，在凭据列表中凭据所在行单击“解除授权”。

----结束

后续操作

您将API授权给指定凭据后，可以通过不同语言的SDK调用此API。

5.9 发布 API

创建完成的API，支持发布到不同的环境。API只有在发布到环境后，才支持被调用。API网关支持查看API发布历史（如版本、发布说明、发布时间和发布环境），并支持回滚到不同的API历史版本。

说明

- 已发布的API，在修改信息后，需要重新发布才能将修改后的信息同步到环境中。
- 同一个API在每个环境中最多记录10条最新的发布历史。

前提条件

已创建环境。

发布 API

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 在“API运行”页面，选择待发布的API，单击“发布”。

步骤6 选择API需要发布到的环境，并填写发布说明。

说明

- 如果API在选择的环境中已发布，再次发布即为覆盖该环境的API。
- 如果在选择的环境时没有自己需要的环境，可以创建一个自己需要的环境。

步骤7 单击“确定”，API发布成功后，“发布”按钮左上角的红色感叹号消失。

已发布的API因为其他原因需要暂停对外提供服务，可以暂时将API从相关环境中下线。该操作将导致此API在指定的环境无法被访问，请确保已经告知使用此API的用户后，选择待下线的API，单击“下线”即可。

----结束

查看发布历史

步骤1 在“API运行”页面，选择待查看发布历史的API。

步骤2 单击“更多 > 发布历史”。

步骤3 在版本所在行，单击“查看版本”，弹出此版本详细信息对话框。

查看API基本信息、API请求、后端请求、入参定义、参数映射、常量参数和返回结果。

步骤4 如果想要设置之前版本为当前版本，则在版本所在行，单击“切换至此版本”，弹出“切换至此版本”对话框。

单击“确定”，完成版本的切换。此时版本号旁边显示“当前版本”，说明设置成功。

API调用者调用此API时，API参数为“当前版本”设置的参数，不是最后一次编辑保存的API参数。

例如，2018年8月1日发布在RELEASE环境的API匹配模式设置为“绝对匹配”，2018年8月20日修改API匹配模式设置为“前缀匹配”，并发布到RELEASE环境。然后设置2018年8月1日发布的版本为当前版本，此时API调用者调用此API时，API的匹配模式为“绝对匹配”。

----结束

发布 API 相关的 FAQ

对API的修改是否需要重新发布?

API发布到RELEASE环境可以正常访问，发布到非RELEASE环境无法访问?

API发布到不同环境后，会调用不同的后端服务吗?

5.10 下线 API

已发布的API因为其他原因需要暂停对外提供服务，可以暂时将API从相关环境中下线。

须知

该操作将导致此API在指定的环境无法被访问，请确保已经告知使用此API的用户。

前提条件

- 已创建API分组和分组内的API。
- API已发布到该环境。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*API分组名称*，进入API分组详情页面。

- 单个下线API。在左侧选择API，然后在右上角单击“下线”，弹出“下线API”对话框。
- 批量下线API，最多同时下线1000个API。单击“批量操作”，选择API，然后单击下线按钮，弹出“下线API”对话框。

步骤5 选择API需要下线的环境，单击“确定”，完成API下线。

----结束

后续操作

您将API下线后，可以通过删除API，释放此API所占用的资源。

5.11 导入 API

API网关支持导入Swagger 2.0定义的API到已有的API分组或新的API分组。Swagger是基于OpenAPI规范构建的开源工具，可以帮助您设计、构建、记录以及使用Rest API。

导入API支持单个API导入和批量API导入，主要取决于Swagger文件中包含的API数量。

前提条件

- 导入API前，您需要在导入的API定义文件中补全《API网关开发指南》的“扩展定义”。如果“扩展定义”中未包含需要的定义，请提前在API网关中创建。
- 导入API前，请确保API分组和API的配额满足需求。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API列表”。

步骤4 单击导入API，具体操作请参考**导入API设计文件**。

----结束

后续操作

将导入成功的API**发布到环境**中，以便API调用者调用。

5.12 导出 API

导出JSON或YAML格式的API。API网关支持单个API导出和批量API导出。

操作步骤

步骤1 **登录API网关控制台**。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。单击*分组名称*然后单击“导出”。

或在左侧导航栏选择“API管理 > API列表”，单击“导出API”。

步骤4 设置导出参数。

表 5-18 导出 API

信息项	描述
API分组	选择待导出API所在的API分组。
运行环境	选择待导出API所在的环境。
API	默认导出API分组所在环境的所有的API，如果需要导出个别API，单击“自定义导出API”，勾选需要导出的API名称。
API定义范围	● 基础定义：包括API前端请求定义和响应定义，不包括后端服务定义。其中API前端请求定义除了Swagger规范定义项外，还包括API网关的一些Swagger扩展字段。 ● 全量定义：包括API前端请求定义、后端服务定义和响应定义。 ● 扩展定义：包括API前端请求定义、后端服务定义和响应定义，还包括API关联的流量控制、访问控制等策略对象的定义。
导出格式	选择JSON或YAML。
自定义版本	为导出的API自定义版本号，如果没有指定版本号，默认使用当前时间。

步骤5 单击“导出”，右侧显示导出结果，并自动下载文件。

----结束

5.13 查看 API 列表

API列表支持查看当前实例下所有的API，包含URL、运行环境、安全认证等信息。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 您可以管理当前实例下的所有API，支持编辑、发布、调试等操作。

步骤4 在左侧导航栏选择“API管理 > API列表”，进入到API列表页面。

步骤5 单击*API名称*，进入API所属分组的详情页面，“创建API”、“域名管理”、“环境变量”等操作可参考上文章节了解详情。

----结束

5.14 支持 HTTP2.0

API网关支持HTTP/2（超文本传输协议第2版）访问协议，通常称之HTTP2.0。拥有二进制格式编码、多路复用共享连接和请求头压缩的能力，改进传输性能，实现低延迟和高吞吐量。

说明

- 由于HTTP2.0是强依赖网络稳定性的，建议用户在使用HTTP2.0时使用比较稳定的网络场景，而且客户端须支持HTTP2.0。
- 如果当前实例不支持HTTP2.0，请联系技术支持升级实例。

- Binary Format二进制格式

  HTTP1.x以文本的形式传输，而HTTP2.0将所有传输信息分割为更小的消息和帧，并对它们采用二进制格式编码。相对于字符串（文本）解析，二进制格式解析更方便且不易出错，提升传输性能。

- MultiPlexing多路复用

  在二进制格式的基础上，HTTP2.0不再依赖多个连接去实现并行处理、发送请求及响应。

  同域名下所有通信都在单个连接上完成；每个连接可以承载任意数量的消息；消息由一个或多个帧组成，多个帧之间可以乱序发送，最后可以根据帧首部的流标识重新组合。从而实现低延迟，提升效率。

- Header压缩

  HTTP2.0使用encoder来减少需要传输的Header大小，客户端与服务端各自保存一份Header fields表，避免重复header传输，减少传输大小，实现高吞吐量。

6 API 策略

6.1 创建策略

通过策略的方式，为API提供灵活的控制策略和扩展能力。

须知

策略参数会明文展示，为防止信息泄露，请谨慎配置。

前提条件

- 一个API只能绑定一个相同类型的策略。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建策略

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 单击需要创建的策略类型。

- **插件策略**

  在创建策略弹窗中配置策略信息。

表 6-1 策略配置

信息项	描述
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。
策略类型	选择策略的类型，不同类型的策略提供不同扩展能力。 **说明** 如果您要使用以下的某个策略在当前实例中不支持，请联系技术支持升级实例到最新版本。 – **跨域资源共享策略**：为API的跨域访问提供指定预检请求头和响应头、自动创建跨域预检请求API的能力。 – **HTTP响应头管理策略**：可以自定义HTTP响应头，在返回的API响应中指定配置的响应头。 – **流量控制2.0策略**：可以限制单位时间内API的被调用次数，支持参数流控、基础流控和基于基础流控的特殊流控。 – **Kafka日志推送策略**：Kafka日志推送策略提供了把API的详细调用日志推送到Kafka的能力，方便用户获取API的调用日志信息。 – **断路器策略**：断路器是API网关在后端服务出现性能问题时保护系统的内置机制。
描述	填写策略的描述信息。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。 不同的策略类型，策略内容的配置不同： – **跨域资源共享策略说明** – **HTTP响应头管理策略说明** – **流量控制2.0策略说明** – **Kafka日志推送策略说明** – **断路器策略说明**

- **传统策略**

  不同的策略类型，策略内容的配置不同：

  – **流量控制策略说明**
  – **访问控制策略说明**
  – **签名密钥策略说明**

步骤6 单击“确定”。

策略创建后，您还需要**为API绑定策略**，才能使策略对API生效。

----结束

为 API 绑定策略

步骤1 单击*策略名称*，进入策略详情。

步骤2 在“关联API”区域选择环境后，单击“绑定API”。

步骤3 筛选API分组，勾选所需的API。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

6.2 跨域资源共享策略说明

出于安全性考虑，浏览器会限制从页面脚本内发起的跨域请求，此时页面只能访问当前域的资源。CORS允许浏览器向跨域服务器发送XMLHttpRequest请求，从而实现跨域访问。更多跨域访问的说明请参见**访问控制策略说明**。

跨域资源共享策略为跨域访问提供指定预检请求头和响应头、自动创建跨域预检请求API的扩展能力，可快速、灵活的实现API的跨域访问。

说明

如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。

使用限制

- 已了解**前提条件**。
- 同一API分组下，相同请求路径的所有API，只能绑定同一个跨域资源共享策略。
- 如果API开启了“支持CORS”功能的同时，也绑定了跨域资源共享策略，则以绑定的策略为准。
- 如果某个请求路径下有OPTIONS方法的API，则该请求路径下的所有API均不允许绑定跨域资源共享策略。
- **为API绑定策略**时，API的请求方法必须为allow_methods中允许的请求方法。

配置参数说明

表 6-2 配置参数说明

信息项	描述
Allowed Origins	Access-Control-Allow-Origin响应头，指定允许访问API的外域URI，多个URI之间使用英文逗号隔开。 对于未携带身份凭证的请求，可以把参数值设置为“*”，表示允许来自所有域的访问请求。
Allowed Methods	Access-Control-Allow-Methods响应头，指定允许使用的HTTP请求方法，多个请求方法之间使用英文逗号隔开。

信息项	描述
Allowed Headers	Access-Control-Allow-Headers响应头，指定XMLHttpRequest请求中允许携带的请求头字段，多个请求头之间使用英文逗号隔开。 其中，简单请求头Accept、Accept-Language、Content-Language、Content-Type（取值仅限为application/x-www-form-urlencoded、multipart/form-data、text/plain时）默认允许在请求中携带，无需在该参数中设置。 **说明** ● 创建跨域资源共享策略时，默认不配置Allowed Headers，不允许跨域请求携带任何自定义请求头。 ● 配置Allowed Headers为“*”，表示允许跨域请求头携带所有请求头。
Exposed Headers	Access-Control-Expose-Headers响应头，指定XMLHttpRequest请求响应中允许携带的响应头字段，多个响应头之间使用英文逗号隔开。 其中，基本响应头Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma默认允许在响应中携带，无需在该参数中设置。 **说明** ● 创建跨域资源共享策略时，默认不配置Exposed Headers，不允许浏览器的JavaScript代码解析跨域访问获得的响应头内容（除XMLHttpRequest对象的getResponseHeader()方法获得的基本响应头，Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma）。 ● 配置Exposed Headers为“*”，表示允许浏览器的JavaScript代码解析跨域访问获得的所有响应头内容。
Maximum Age	Access-Control-Max-Age响应头，指定本次预检请求的有效期，单位为秒。在有效期内，无需再次发出预检请求。
Allowed Credentials	Access-Control-Allow-Credentials响应头，定XMLHttpRequest请求中是否允许携带Cookie。 ● 开关开启表示允许。 ● 开关关闭表示不允许。

脚本配置示例

```
{
  "allow_origin": "*",
  "allow_methods": "GET,POST,PUT",
  "allow_headers": "Content-Type,Accept,Accept-Ranges,Cache-Control",
  "expose_headers": "X-Request-Id,X-Apig-Latency",
  "max_age": 86400,
  "allow_credentials": true
}
```

6.3 HTTP 响应头管理策略说明

API响应是指API网关返回客户端的响应，HTTP响应头是API响应中的一部分。您可以自定义HTTP响应头，在返回的API响应中指定您配置的响应头。

说明

如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。

使用限制

无法修改API网关增加的系统响应头（x-apig-*，x-request-id等），包括API网关提供的CORS功能增加的响应头。

配置参数说明

表 6-3 配置参数说明

信息项	描述
Name	响应头名称。每个策略中不能添加重复名称的响应头（不区分大小写），且最多添加10条响应头。
Value	响应头的值。当“Action”为“Delete”时响应头的值不生效，可为空。

信息项	描述
Action	响应头操作，您可以覆盖、添加、删除、跳过或新增指定的响应头。 **Override**：覆盖 ● 当API响应中存在指定的响应头时，使用当前响应头的值覆盖已有响应头的值。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，该操作只会按当前响应头的值返回一条响应头记录。 ● 当API响应中不存在指定的响应头时，添加当前响应头。 **Append**：添加 ● 当API响应中存在指定的响应头时，将当前响应头的值添加到已有响应头值之后，用逗号分隔。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，会将多个响应头的值用“，”拼接后，再添加当前响应头的值。 ● 当API响应中不存在指定的响应头时，添加当前响应头。 **Delete**：删除 ● 当API响应中存在指定的响应头时，删除当前响应头。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，删除所有相同名称的响应头。 **Skip**：跳过 ● 当API响应中存在指定的响应头时，跳过当前响应头。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，均不作处理直接返回。 ● 当API响应中不存在指定的响应头时，添加当前响应头。 **Add**：新增 无论API响应中是否存在指定的响应头，都添加当前响应头。

脚本配置示例

```
{
    "response_headers": [
        {
            "name": "test",
            "value": "test",
            "action": "append"
        },
        {
            "name": "test1",
            "value": "test1",
            "action": "override"
        }
```

```
  ]
}
```

6.4 流量控制 2.0 策略说明

流量控制2.0策略可以限制单位时间内API的被调用次数，支持参数流控、基础流控和基于基础流控的特殊流控。

- 基础流控

  可以对API、用户、凭据、源IP进行多维度流控，与已有的流量控制策略说明功能一致但不兼容。

- 参数流控

  支持根据Header、Path、Method、Query以及系统变量中的参数值进行自定义流控。

- 基于基础流控的特殊流控

  对某个凭据或租户进行特定的流控。

说明

如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。

使用限制

- 如果一个API绑定流量控制后，继续绑定参数控制策略，流量控制会失效。
- 参数流控的规则最多可定义100个。
- 策略内容最大长度65535。

配置参数说明

表 6-4 配置参数说明

参数	配置说明
流控类型	推荐使用高性能流控。 ● 高精度流控：高并发场景下实例内部会有一定的性能损耗，适用于并发量较小的场景。 ● 高性能流控：高并发场景下实例内部性能损耗较小，单位时间内会偶现较小的误差值，适用于并发量较大的场景。 ● 单机流控：实例的每个节点各自进行流控，高并发场景下实例内部性能损耗最小，单位时间内会存在一定的误差值，适用于并发量更大的场景。
策略生效范围	● 单个API生效 对单个API进行流量统计和控制。 ● API共享生效 对绑定了该策略的所有API进行总流量统计和控制。

参数	配置说明
时长	流量限制的时长。 ● 与“API流量限制”配合使用，表示单位时间内的单个API请求次数上限。 ● 与“用户流量限制”配合使用，表示单位时间内的单个用户请求次数上限。 ● 与“凭据流量限制”配合使用，表示单位时间内的单个凭据请求次数上限。 ● 与“源IP流量限制”配合使用，表示单位时间内的单个IP地址请求次数上限。
API流量限制	单个API被调用次数上限。 与“时长”配合使用，表示单位时间内的单个API请求次数上限。
用户流量限制	单个用户调用API次数上限，如果API认证方式为IAM认证，用户流量根据项目ID来限制；如果API认证方式为APP认证，用户流量根据帐号ID来限制。帐号ID和项目ID请参考下文“特殊租户”配置说明。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个用户请求次数上限。 ● 如果主帐号下有多个子用户访问API，按主帐号累计的调用次数进行限制。
凭据流量限制	单个凭据调用API次数上限，仅适用于API的安全认证方式为APP认证时。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个凭据请求次数上限。
源IP流量限制	单个IP地址调用API次数上限。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个IP地址请求次数上限。
参数流控配置	参数流控配置开关。开启后，以参数维度进行流控限制。
定义参数	定义用于规则匹配的参数。 ● 参数位置：用于规则匹配的参数位置。 – path：API请求的URI，系统默认配置。 – method：API请求方法，系统默认配置。 – Header：请求头的key值。 – Query：QueryString的key值。 – System：系统参数。 ● 参数：用于判断与规则匹配中的参数值是否匹配。

参数	配置说明
定义规则	定义规则的匹配条件，以及API流量限制和时长。 单击“添加规则”，可添加多个规则。 ● 规则匹配 单击 ，可添加多个条件表达式，选择“定义参数”中的参数名和判断条件，以及输入参数值。 – =为等于 – !=为不等于 – pattern为正则表达式 – enum为枚举值，多个参数值之间用英文逗号分隔 ● API流量限制 API调用次数的最大值。 ● 时长 定义规则的流量控制时长，如果此处不配置时长，规则的流量控制时长以“策略基本信息”的时长为准。 例如，在“定义参数”中添加参数“Host”，参数位置选择“Header”；在“定义规则”中添加一条规则，匹配条件设置成“Host = www.abc.com”，API流量限制为10，时长为60s。表示在60s内，对于请求头域中Host参数等于“www.abc.com”的API，且API调用次数达到10，参数流控生效。
特殊流控配置	特殊流控配置开关。开启后，“基础流控”的用户流量限制/凭据流量限制与“特殊流控”的特殊租户/特殊凭据共同作用时，以特殊流控值为准。
特殊租户	租户ID为帐号ID或项目ID。 ● 绑定APP认证的API时，租户ID为项目ID，请参考《API网关接口参考》中的“获取项目ID”章节。 ● 绑定IAM认证的API时，租户ID为帐号ID，不支持细分到IAM用户维度，请参考《API网关接口参考》中的“获取帐号名和帐号ID”章节。 阈值为单位时间内，此租户访问API的最大值，不超过“基础流控”的API流量限制值。
特殊凭据	选择已有凭据，阈值为单位时间内，此凭据访问API的最大值，不超过“基础流控”的API流量限制值。

脚本配置示例

```
{
  "scope": "basic",
  "default_interval": 60,
  "default_time_unit": "second",
  "api_limit": 100,
  "app_limit": 50,
  "user_limit": 50,
  "ip_limit": 20,
  "specials": [
```

```
    {
      "type": "app",
      "policies": [
        {
          "key": "e9230d70c749408eb3d1e838850cdd23",
          "limit": 10
        }
      ]
    },
    {
      "type": "user",
      "policies": [
        {
          "key": "878f1b87f71c40a7a15db0998f358bb9",
          "limit": 10
        }
      ]
    }
  ],
  "algorithm": "counter",
  "parameters": [
    {
      "id": "3wuj354lpptv0toe0",
      "value": "reqPath",
      "type": "path",
      "name": "reqPath"
    },
    {
      "id": "53h7e7j11u38l3ocp",
      "value": "method",
      "type": "method",
      "name": "method"
    },
    {
      "id": "vv502bnb6g40td8u0",
      "value": "Host",
      "type": "header",
      "name": "Host"
    }
  ],
  "rules": [
    {
      "match_regex": "[\"Host\",\"==\",\"www.abc.com\"]",
      "rule_name": "u8mb",
      "time_unit": "second",
      "interval": 2,
      "limit": 5
    }
  ]
}
```

6.5 Kafka 日志推送策略说明

支持收集已开放API的调用日志信息。Kafka日志推送策略提供了把API的详细调用日志推送到Kafka的能力，方便用户获取API的调用日志信息。

说明

如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。

使用限制

- 同一个APIG实例内最多可创建5个Kafka日志推送策略。
- API绑定Kafka日志推送策略后，性能将损耗30%。

配置参数说明

表 6-5 配置参数

参数	配置说明
策略基本信息	
Broker地址	填写目标Kafka的连接地址，建立连接关系。多个地址间以英文逗号（,）隔开。
Topic主题	填写目标Kafka上报日志的主题。
Key	填写日志的Key值，表示日志存储在Kafka的指定分区，可以当成有序消息队列使用。如果Key为空，则日志分布式存储在不同的消息分区。
失败重试分配	日志推送到Kafka失败后的重试配置。 ● 重试次数：失败后的重试次数，范围为0-5次。 ● 重试间隔时间：失败后的重试时间间隔，范围为1-10秒。
SASL配置信息	
安全协议	连接目标Kafka所使用的安全协议。 ● PLAINTEXT：默认接入点的用户认证协议。 ● SASL_PLAINTEXT：SASL用户认证协议。 ● SASL_SSL：SSL用户认证协议。
消息收发机制	目标Kafka的消息收发机制，默认为PLAIN。
SASL用户名	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** SASL或SSL认证所使用的用户名。
SASL用户密码	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** SASL或SSL认证所使用的用户密码。
确认SASL用户密码	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** 填写与SASL用户密码一样的值。
证书内容	**仅当“安全协议”选择“SASL_SSL”时需配置。** SSL认证所使用的CA证书内容。
元数据配置信息	

参数	配置说明
系统元数据	推送的日志中，需要携带的系统字段信息。 其中，start_time、request_id、client_ip、request_time、http_status、scheme、request_method、host、uri、upstream_addr、upstream_status、upstream_response_time、http_x_forwarded_for、http_user_agent和error_type字段信息默认在日志中携带，其他系统字段需勾选后才携带。
请求数据	推送的日志中，需要携带的API请求信息。 ● 日志包含请求头域信息：勾选后，需填写日志中要携带的请求Header参数。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 ● 日志包含请求QueryString信息：勾选后，需填写日志中要携带的请求Query参数信息。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 ● 日志包含请求Body体信息：勾选后，日志中会携带API请求的Body体信息。
响应数据	推送的日志中，需要携带的API响应信息。 ● 日志包含响应头域信息：勾选后，需填写日志中要携带的响应Header参数。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 ● 日志包含响应Body体信息：勾选后，日志中会携带响应Body体信息。
自定义认证配置	推送的日志中，需要携带的自定义认证信息。 ● 前端：填写日志中要携带的前端自定义认证的响应字段信息，多个字段间使用英文逗号（,）分隔。 ● 后端：填写日志中要携带的后端自定义认证的响应字段信息，多个字段间使用英文逗号（,）分隔。

6.6 断路器策略说明

断路器是API网关在后端服务出现性能问题时保护系统的内置机制。当API的后端服务出现连续N次超时或者时延较高的情况下，会触发断路器的降级机制，向API调用方返回固定错误或者将请求转发到指定的降级后端。当后端服务恢复正常后，断路器关闭，请求恢复正常。

说明

如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。

配置参数说明

表 6-6 配置参数

参数	配置说明
策略生效范围	● 单个API生效 对单个API进行控制。 ● API共享生效 对绑定了该策略的所有API进行控制。
断路器类型	选择断路器的触发类型。 ● 超时降级：断路器以后端服务超时作为触发条件。 ● 匹配条件降级：断路器以“匹配条件”中的设置作为触发条件。
条件模式	选择断路器的触发模式。 ● 计数器：在时间窗内满足触发条件的请求次数达到设定阈值，则立即触发断路器。 ● 百分比：在时间窗内满足触发条件的请求率达到设定阈值，时间窗结束后触发断路器。
匹配条件	**仅当“断路器类型”选择“匹配条件降级”时需配置。** 配置断路器的触发条件。 ● 响应错误码：后端响应状态码符合设定值，则该后端请求满足触发条件。 ● 触发降级响应时延：后端响应时延超过设定值，则该后端请求满足触发条件。
时间窗（秒）	断路器的触发次数统计时间窗，与“阈值”或“最小百分比”参数配合使用，当时间窗内的触发次数达到设定阈值或百分比，则触发断路器。
阈值（次）	**仅当“条件模式”选择“计数器”时需配置。** 断路器的触发阈值，与“时间窗”参数配合使用。在时间窗内，满足触发条件的后端请求次数达到阈值，则触发断路器。 **说明** 断路器策略是按单个网关组件分开触发，如果API网关存在多个网关组件，则各个网关组件的触发统计分开计数。 如果某个网关组件在时间窗内的触发次数超过阈值，则发送到该网关组件上的请求会触发断路器，其他未超过阈值的网关组件依然正常转发请求。 您可以在API网关实例控制台的“实例信息”页面，在“出私网IP”下查看网关组件的IP个数，一个IP表示为一个网关组件。
最小调用次数	**仅当“条件模式”选择“百分比”时需配置。** 时间窗内触发断路器的API最小调用次数。如果时间窗内API的总调用次数小于该值，则不触发断路器。

参数	配置说明
最小百分比（%）	**仅当“条件模式”选择“百分比”时需配置。** 断路器的触发阈值，与“时间窗”参数配合使用。当时间窗内的满足触发条件的后端请求百分比达到阈值，则触发断路器。
开启时长（秒）	断路器开启的持续时间，断路器开启时间达到该值后将关闭。
后端降级策略	后端降级策略开关。 ● 开启：触发降级的API将把请求转发到指定后端服务。 ● 关闭：触发降级的API不会把请求转发到任何后端服务，直接返回服务不可用的错误信息。

参数	配置说明
后端策略类型	**仅当“后端降级策略”开启时需配置。** 断路器开启后，后端请求的转发策略类型。 ● Mock：把配置的响应结果作为后端服务响应固定返回。 – Mock自定义返回码：后端服务响应的状态码。 – Mock返回结果：后端服务响应的Body信息，JSON格式。 – 响应头参数：后端服务响应的Header参数。 ● HTTP&HTTPS：把后端服务请求转发给指定HTTP&HTTPS后端服务。 – 负载通道：是否使用负载通道访问后端服务。如果选择“使用”，您需要提前**创建负载通道**。 – 后端URL：配置要转发的后端服务请求地址。 – 后端超时(ms)：后端服务请求的超时时间，默认为5000ms。 ● FunctionGraph：把后端服务请求转发给指定函数。 – 函数URN：函数请求的唯一标识。单击“添加”，添加作为后端服务的函数URN。 – 函数名：选择函数URN后自动配置。 – 版本：选择要使用的函数版本。 – 调用类型：选择函数的调用类型。 Synchronous：表示同步调用，后端函数服务收到调用请求后立即执行并返回调用结果，客户端发送请求后同步等待，收到后端响应后关闭连接。 Asynchronous：表示异步调用，后端函数服务收到调用请求后将请求排队，执行成功后返回调用结果，服务端在空闲的情况下会逐个处理排队的请求，客户端不关注请求调用的结果。 – 后端超时(ms)：后端服务请求的超时时间，默认为5000ms。 ● Passthrough：把后端服务请求转发给API的原后端服务。 单击“添加参数”，可为转发给后端服务的请求添加请求头参数。

参数	配置说明
降级参数配置	降级参数配置开关。开启后可为断路器自定义规则，API请求优先匹配自定义规则中的触发条件和降级策略，仅当未匹配到自定义规则时才执行上方配置的默认触发条件和降级策略。 ● 如果匹配到自定义规则，则执行规则内配置的触发条件和降级策略。如果匹配到的自定义规则内未配置触发条件或降级策略，则执行上方配置的默认触发条件或降级策略。 ● 如果未匹配到自定义规则，则执行上方配置的默认触发条件和降级策略。
定义参数	定义用于规则匹配的参数。 ● 参数位置：参数在API请求中的位置。 ● 参数：用于做规则匹配的参数名。 系统默认包含reqPath（请求路径）和method（请求方法）参数。单击“添加参数”，可添加其他匹配参数。
定义规则	自定义断路器的匹配规则。单击“添加规则”，可添加规则，系统根据从上到下的顺序匹配规则，可通过上下移动调整规则优先级。 ● 匹配条件：单击“ ”编辑匹配条件表达式。如果表达式数量大于等于3个，可通过“转子层级”对表达式进行分层设置。 – =为等于 – !=为不等于 – pattern为正则表达式 – enum为枚举值，多个参数值之间用英文逗号分隔 ● 触发条件和后端降级策略配置可参考上方的默认触发条件和降级策略配置。 例如，开启“降级参数配置”，按顺序添加“rule01”和“rule02”规则，“rule01”关闭“触发条件配置”并且开启“后端降级策略”，“rule02”两者都开启。断路器优先判断“rule01”匹配条件，如果匹配则会按照上方配置的默认触发条件开启断路器（rule01内未配置触发条件），并执行rule01内的后端降级策略。如果不匹配则会继续判断“rule02”，以此类推。

脚本配置示例

```
{
  "breaker_condition":{
    "breaker_type":"timeout",
    "breaker_mode":"counter",
    "unhealthy_threshold":30,
    "time_window":15,
    "open_breaker_time":15,
    "unhealthy_percentage":51,
    "min_call_threshold":20
```

```
  },
  "scope":"share",
  "downgrade_default":{
    "type":"http",
    "passthrough_infos":null,
    "func_info":null,
    "mock_info":null,
    "http_info":{
      "isVpc":false,
      "vpc_channel_id":"",
      "address":"10.10.10.10",
      "scheme":"HTTP",
      "method":"GET",
      "path":"/demo",
      "timeout":5000
    },
    "http_vpc_info":null
  },
  "downgrade_parameters":[
  {
    "name":"reqPath",
    "type":"path",
    "value":"path",
    "disabled":true,
    "focused":true,
    "id":"92002eqbpilg6g"
  },
  {
    "name":"method",
    "type":"method",
    "value":"method",
    "disabled":true,
    "focused":true,
    "id":"tuvxetsdqvcos8"
  }],
  "downgrade_rules":[
  {
    "rule_name":"rule-test1",
    "parameters":[
      "reqPath",
      "method"
    ],
    "match_regex":"[\"reqPath\",\"==\",\"/test\"]",
    "downgrade_backend":{
      "type":"mock",
      "passthrough_infos":null,
      "func_info":null,
      "mock_info":{
        "status_code":200,
        "result_content":"{status: ok}",
        "headers":[]
      },
      "http_info":null,
      "http_vpc_info":null
    },
    "breaker_condition":{
      "breaker_type":"timeout",
      "breaker_mode":"percentage",
      "unhealthy_threshold":30,
      "time_window":15,
      "open_breaker_time":15,
      "unhealthy_percentage":51,
      "min_call_threshold":20
    }
  }]
}
```

6.7 流量控制策略说明

流量控制支持从用户、凭据和时间段等不同的维度限制对API的调用次数，保护后端服务。支持按分/按秒粒度级别的流量控制。为了提供持续稳定的服务，您可以通过创建流控策略，针对部分API进行流量控制。

使用限制

- API添加流控策略相当于流控策略同步绑定了API。同一个环境中，一个API只能被一个流控策略绑定，但一个流控策略可以绑定多个API。
- 如果API未绑定流控策略，流控限制值为实例“配置参数”中“ratelimit_api_limits”的参数运行值。

配置参数说明

表 6-7 配置参数说明

信息项	描述
策略名称	API流控策略名称。
类型	分“基础流控”和“共享流控”两类。 ● 基础流控针对**单个**API进行流量统计和控制； ● 共享流控针对绑定了该策略的**所有**API进行总流量统计和控制。
时长	流量限制的时长。 ● 与“API流量限制”配合使用，表示单位时间内的单个API请求次数上限。 ● 与“用户流量限制”配合使用，表示单位时间内的单个用户请求次数上限。 ● 与“凭据流量限制”配合使用，表示单位时间内的单个凭据请求次数上限。 ● 与“源IP流量限制”配合使用，表示单位时间内的单个IP地址请求次数上限。
API流量限制	单个API被调用次数上限。 与“时长”配合使用，表示单位时间内的单个API请求次数上限。
用户流量限制	单个用户调用API次数上限，**仅在API的安全认证方式为APP认证或IAM认证时适用**。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个用户请求次数上限。 ● 如果主帐号下有多个子用户访问API，按主帐号累计的调用次数进行限制。

信息项	描述
凭据流量限制	单个凭据调用API次数上限，**仅在API的安全认证方式为APP认证时适用**。 ● 不超过“用户流量限制”和“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的凭据请求次数上限。
源IP流量限制	单个IP地址调用API次数上限。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的IP地址请求次数上限。
描述	关于控制策略的描述。

后续操作

- 如果需要对某个凭据进行流量控制，可以在“流量控制策略”中为凭据绑定流量控制策略。绑定后，该凭据的流量受特殊应用的阈值限制，而API流量和用户流量仍受流量控制策略限制。
- 如果需要对某个租户进行流量控制，可以在“流量控制策略”中为租户绑定流量控制策略。绑定后，该租户的流量受特殊租户的阈值限制，而API流量和用户流量仍受流量控制策略限制。

为凭据绑定流量控制策略

已创建凭据，或已获取其他凭据ID。

步骤1 在流控策略详情页面，单击“特殊应用”页签，进入特殊应用页面。

步骤2 单击“添加特殊应用”，弹出“添加特殊应用”对话框。

步骤3 通过以下两种方式，添加特殊应用。

- 添加已有应用：单击“已有应用”，选择已有凭据，输入阈值。
- 添加其他应用：单击“其他”，输入其他用户的凭据ID和阈值。

说明

特殊应用流控值和凭据流量限制值共同作用时，以特殊应用流控值为准。

例如：API流量限制值为10，凭据流量限制值为3，时长为1分钟，特殊应用（应用A）流控值为2，特殊应用（应用B）流控值为4，应用A在1分钟内最多可以访问绑定了该流控策略的API 2次，应用B在1分钟内最多可以访问绑定了该流控策略的API 4次。

----结束

为租户绑定流量控制策略

步骤1 在流控策略详情页面，单击“特殊租户”，进入特殊租户页面。

步骤2 单击“添加特殊租户”，弹出“添加特殊租户”对话框。

步骤3 输入租户信息。

表 6-8 特殊租户信息

信息项	描述
租户ID	获取的帐号ID或项目ID，请参考表6-4中的“特殊租户”说明。
阈值	固定时间段内，此租户访问API的最大值。 不能超过API流量限制值。

步骤4 单击“确定”，完成特殊租户的添加。

说明

特殊租户流控值和用户流量限制值共同作用时，以特殊租户流控值为准。

例如：API流量限制值为10，用户流量限制值为3，时长为1分钟，特殊租户（租户ID为A）流控值为2，特殊租户（租户ID为B）流控值为4，租户A在1分钟内最多可以访问绑定了该流控策略的API 2次，租户B在1分钟内最多可以访问绑定了该流控策略的API 4次。

----结束

6.8 访问控制策略说明

访问控制策略是API网关提供的API安全防护组件之一，主要用来控制访问API的IP地址和帐户，您可以通过设置IP地址或帐户的黑白名单来禁止/允许某个IP地址/帐号名/帐号ID访问API。

访问控制策略和API本身是相互独立的，只有将访问控制策略绑定API后，访问控制策略才对绑定的API生效。

使用限制

- 同一个API在同一个环境中只能绑定一个相同限制类型的访问控制策略，一个访问控制策略可以绑定多个API。

配置参数说明

表 6-9 配置参数说明

信息项	描述
策略名称	访问控制策略的名称。
类型	控制访问API的类型。 ● IP地址：限制调用API的IP地址。 ● 帐号名：仅适用**IAM认证**类型的API，限制调用API的帐号名。仅支持配置帐号名，对帐号名及帐号名下的IAM用户名做限制，不支持配置IAM用户名。

信息项	描述
动作	包括“允许”和“禁止”。 和“类型”配合使用，允许/禁止访问API的IP地址/帐号名/帐号ID。
IP地址	**仅当“类型”为“IP地址”时需要配置。** 输入允许或者禁止访问API的IP地址，或IP地址范围。 **说明** 允许或禁止访问的IP地址条数，分别可以配置最多100条。
帐号名	**仅当“类型”为“帐号名”时需要配置。** 输入允许或者禁止访问API的帐号名，多个帐号名之间使用英文逗号（,）隔开。 您可以单击控制台右上角的用户名，选择“我的凭证”，在“我的凭证”页面获取用户的帐号名。

6.9 签名密钥策略说明

签名密钥用于后端服务验证API网关的身份，在API网关请求后端服务时，保障后端服务的安全。

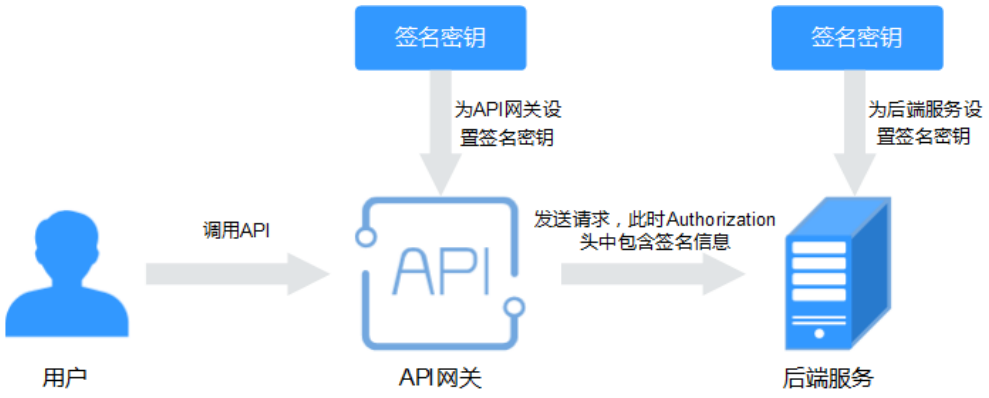
签名密钥由一对Key和Secret组成，签名密钥需要绑定到API才能生效。当签名密钥绑定API后，API网关向后端服务发送此API的请求时，会增加相应的签名信息，此时需要后端服务依照同样方式进行签名，通过比对签名结果和API网关传过来的Authorization头中签名是否一致来校验API的合法性。

使用限制

同一个环境中一个API只能被一个签名密钥绑定，一个签名密钥可以绑定多个API。

使用流程

图 6-1 签名密钥流程图



1. 在控制台创建签名密钥。

2. 将新创建的签名密钥绑定API。
3. API网关将签名后的请求发送到后端服务，此时Authorization头中包含签名信息。后端服务通过不同的开发语言（例如Java、Go、Python、JavaScript、C#、PHP、C++、C等）进行签名，通过比对签名结果和API网关传过来的Authorization头中签名是否一致来校验API的合法性。

配置参数说明

表 6-10 配置参数说明

信息项	描述
密钥名称	自定义名称，用于识别不同的密钥。
类型	选择签名密钥的认证类型，可选择“HMAC”、“Basic Auth”、“AES”。
签名算法	选择aes的签名算法，包含以下两种： ● aes-128-cfb ● aes-256-cfb
Key	根据选择的密钥类型，填写不同的密钥信息。 ● HMAC：填写APP认证所使用密钥对的Key。 ● Basic Auth：填写basic认证所使用的用户名。 ● aes：填写aes认证所使用的密钥key。 ● Public Key：填写public_key认证所使用的公钥。
Secret	根据选择的密钥类型，填写不同的密钥信息。 ● HMAC：填写APP认证所使用密钥对的Secret。 ● Basic Auth：填写basic认证所使用的密码。 ● aes：填写aes认证所使用的向量。 ● Public Key：填写Public Key认证所使用的私钥。
确认Secret	填写与Secret一致的值。

验证签名结果

参考《API网关开发指南》的“对后端服务进行签名”章节对后端服务进行签名，比对签名结果和API网关传过来的Authorization头中签名是否一致来校验API的合法性。

6.10 自定义认证

自定义认证包含两种认证：前端自定义认证和后端自定义认证。

- 前端自定义认证：如果您希望使用自己的认证系统，而不是APP认证/IAM认证对API的访问进行认证鉴权时，您可以使用自定义认证，通过您自定义的函数进行认证鉴权。

- 后端自定义认证：当不同的后端服务使用不同的认证系统时，导致您需要为不同的认证系统定制化开发API，而APIG通过自定义认证功能，将多种认证系统集成，简化API开发的复杂度。您只需要在APIG中创建自定义的函数认证，APIG通过此函数对接后端认证系统，获取后端服务的访问授权。

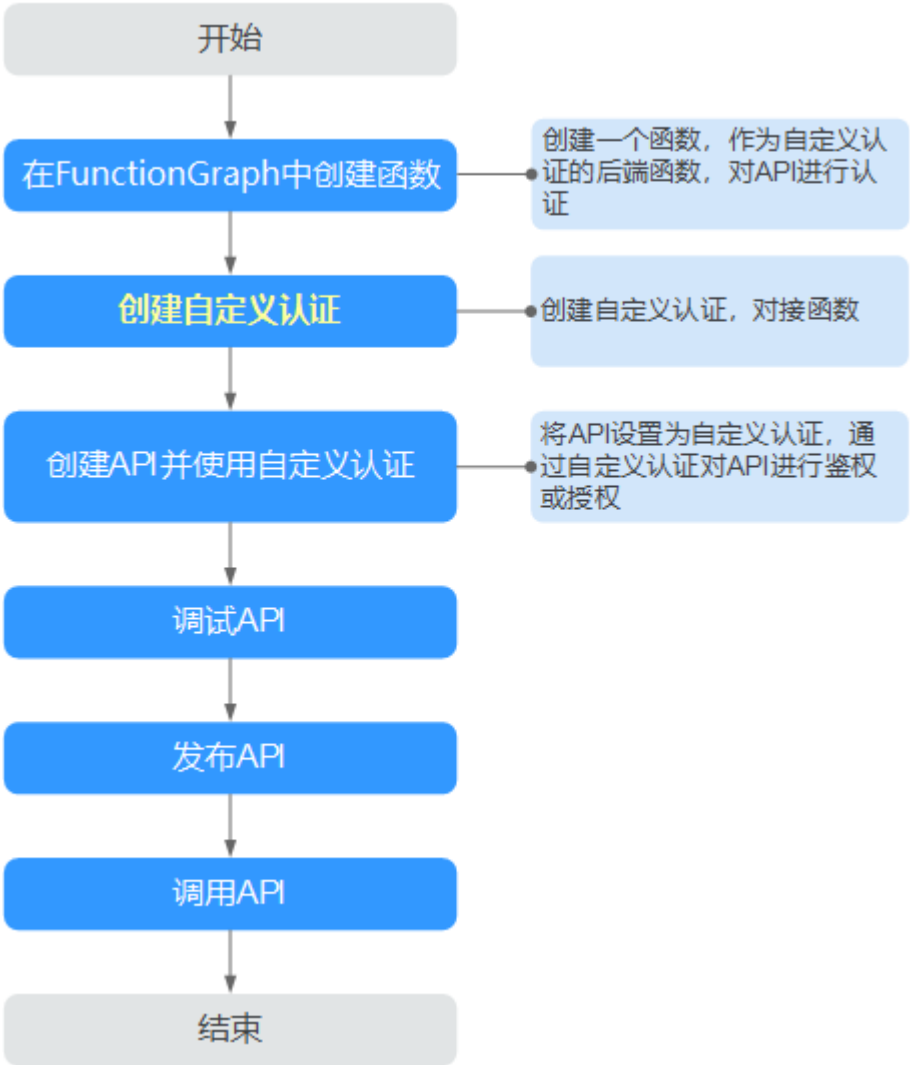
说明

自定义认证依赖函数工作流服务。如果当前Region没有上线函数工作流服务，则不支持使用自定义认证。

自定义认证的具体使用指导，可参考《API网关开发指南》的自定义认证相关章节。

使用自定义认证调用API的流程如下图所示：

图 6-2 使用自定义认证调用 API



前提条件

已在函数工作流服务中完成函数创建。

创建自定义认证

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“自定义认证”页面，单击“创建自定义认证”。

配置自定义认证参数。

表 6-11 自定义认证参数说明

信息项	描述
认证名称	您自定义的认证名称，用于区分不同的自定义认证。
类型	● 前端：对API的访问进行认证鉴权。 ● 后端：对后端服务的访问授权。
函数地址	选择在FunctionGraph中创建的函数。
版本或别名	支持选择函数的版本或别名，函数的版本或别名功能请参考《函数工作流 FunctionGraph用户指南》的“版本管理”和“别名管理”章节。
缓存时间(秒)	设置认证结果缓存的时间。 值为0时代表不缓存，最大支持3600秒。
身份来源	设置用于认证的请求参数。 当“类型”为“前端”，且“缓存时间”不为0时，必须设置此参数。使用缓存时，此参数将作为搜索条件来查询认证结果。
是否发送body	指是否将API请求的body体内容传递给认证函数。body体内容传给函数的方式，与header、query内容传递一致。
用户数据	您自定义的请求参数，APIG调用函数时，与“身份来源”一同作为请求参数。

步骤5 单击“确定”，完成自定义认证的创建。

----结束

6.11 SSL 证书管理

如果API分组中的API支持HTTPS请求协议，则在绑定独立域名后，还需为独立域名添加SSL证书。SSL证书是进行数据传输加密和身份证明的证书。

前提条件

- 仅支持添加pem编码格式的SSL证书。
- 添加的SSL证书仅支持RSA、ECDSA和DSA加密算法。

创建 SSL 证书

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“SSL证书管理”页面，单击“创建SSL证书”。

表 6-12 SSL 证书配置

参数	配置说明
证书名称	填写SSL证书的名称，根据规划自定义。建议您按照一定的命名规则填写SSL证书名称，方便您快速识别和查找。
可见范围	● 当前实例：仅在当前实例下展示此证书。 ● 全局：在所有实例下都会展示此证书。
证书内容	填写pem编码格式的SSL证书内容。 以文本方式打开待添加证书里的PEM格式证书文件（后缀名为“.pem”），将证书内容复制到“证书内容”中即可。 如果证书为非pem编码格式，可参考转换证书为PEM格式进行证书格式转换。
密钥	填写pem编码格式的SSL证书密钥。 以文本方式打开待上传证书里的KEY格式或PEM格式的私钥文件（后缀名为“.pem”或“.key”），将私钥复制到“密钥”中即可。

步骤5 单击“确定”，完成SSL证书的添加。

----结束

转换证书为 PEM 格式

格式类型	转换方式（通过OpenSSL工具进行转换）
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	● 提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 openssl pkcs12 -in cert.pfx -nocerts -out key.pem ● 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。

格式类型	转换方式（通过OpenSSL工具进行转换）
DER	• 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem • 提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

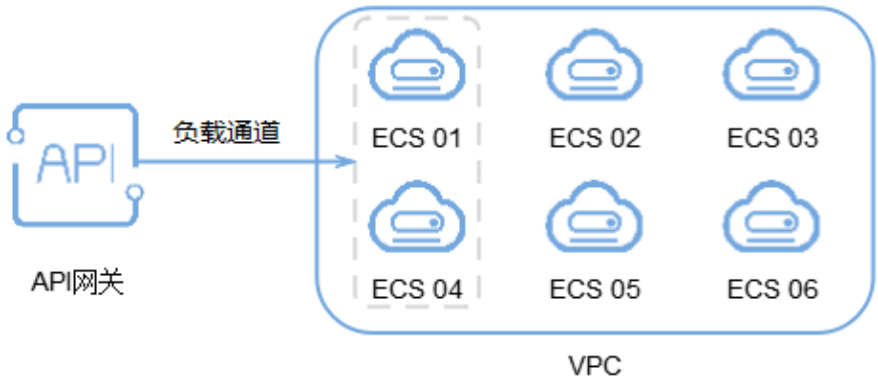
6.12 负载通道

负载通道主要用于将服务通过API网关开放给外部访问。它的优势在于使用VPC的内部子网通信，网络时延更低，同时负载通道具有负载均衡功能，从而实现后端服务的负载均衡。

创建负载通道后，在创建API，且后端服务类型为HTTP/HTTPS时，后端服务地址可以直接使用已创建的负载通道。

例如，负载中包含6台ECS，已创建一条负载通道，其中ECS 01和ECS 04已添加到负载通道中，此时API网关通过负载通道可以直接访问负载中的ECS 01和ECS 04。

图 6-3 通过 API 网关访问负载通道中的 ECS



前提条件

- 用户需要具备VPC Administrator角色权限。

创建负载通道

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 单击“负载通道”页签，进入到负载通道列表页面。

步骤5 单击“创建负载通道”，配置基本信息。

表 6-13 基本信息配置

信息项	描述
通道名称	自定义负载通道名称，用于识别不同的负载通道。
端口	负载通道中主机的端口号，即用户的后端业务端口号。 取值范围为1 ~ 65535。
分发算法	通过分发算法确定请求被发送到哪台主机。 分发算法包含如下几种： ● 加权轮询 ● 加权最小连接 ● 源地址哈希 ● URI哈希

步骤6 配置通道内服务器。

说明

- 待添加的云服务器的安全组必须允许100.125.0.0/16网段访问，否则将导致健康检查失败及业务不通。
- 负载通道支持私网ELB，可通过指定服务器地址配置。

- 选择云服务器。
  a. 单击“创建服务器分组”。
     在弹窗中填写服务器分组信息，单击“确定”。

     表 6-14 服务器分组配置

信息项	描述
分组名称	填写服务器分组的名称，根据规划自定义。建议您按照一定的命名规则填写分组名称，方便您快速识别和查找。
权重	填写服务器分组的权重值，权重值越大，转发到该分组下服务器的请求数量越多。
描述	填写分组的描述信息。

  b. 单击“添加云服务器”。
     在弹窗中，选择子网并勾选要添加的云服务器，单击“确定”。
  c. 配置完成后，进行健康检查配置。
- 指定服务器地址。
  a. 单击“创建服务器分组”。

在弹窗中填写服务器分组信息，单击“确定”。配置参数请参考表6-14。

b. 单击“添加后端服务器地址”，在列表中填写后端服务器地址。

表 6-15 后端服务器配置

信息项	描述
后端服务器地址	填写后端服务器的IP地址。
是否备用节点	开启后对应后端服务器为备用节点，仅当非备用节点全部故障时工作。
端口	填写后端服务器的访问端口号，端口为0时使用负载通道的端口。
启停状态	选择是否启用服务器，只有启用后，请求才会分发到该服务器上。

c. 配置完成后，进行健康检查配置。

步骤7 配置健康检查。

表 6-16 基本信息配置

信息项	描述
协议	使用以下协议，对负载中主机执行健康检查。 ● TCP ● HTTP ● HTTPS 默认为TCP协议。
双向认证	**仅在协议为“HTTPS”时，需要设置。** 开启后，API网关将认证API后端服务。双向认证所需的证书配置说明，请参考配置参数。
路径	**仅在协议不为“TCP”时，需要设置。** 健康检查时的目标路径。
请求类型	● GET ● HEAD
检查端口	健康检查的目标端口。 缺省时，检查端口为负载通道的端口号。
正常阈值	判定负载通道中主机正常的依据为：连续检查x成功，x为您设置的正常阈值。 取值范围为2 ~ 10。缺省值为2。
异常阈值	判定负载通道中主机异常的依据为：连续检查x失败，x为您设置的异常阈值。 取值范围为2 ~ 10。缺省值为5。

信息项	描述
超时时间	检查期间，无响应的时间，单位为秒。 取值范围为2 ~ 30。缺省值为5。
间隔时间	连续两次检查的间隔时间，单位为秒。 取值范围为5 ~ 300。缺省值为10。
HTTP响应码	**仅在协议不为“TCP”时，需要设置。** 检查目标HTTP响应时，判断成功使用的HTTP响应码。

步骤8 单击“完成”，完成负载通道的创建。

----结束

后续操作

创建API，将部署在负载中的后端服务开放API。

6.13 环境管理

API可以同时提供给不同的环境调用，如生产、测试或开发。RELEASE是默认存在的环境，无需创建。

创建环境

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 单击“环境管理”页签。

步骤5 单击“创建环境”，填写环境信息。

表 6-17 环境信息

信息项	描述
环境名称	API环境名称。
描述	环境描述信息。

步骤6 单击“确定”，创建环境。

创建环境成功后，在“环境管理”页面的列表中显示新创建的环境。

----结束

访问环境

通过RESTful API可以访问API默认的RELEASE环境，如果访问其他环境，需要在请求头中添加X-Stage头，内容为环境名。例如访问名为“DEVELOP”的环境，则添加“X-Stage:DEVELOP”。

说明

API网关管理控制台的“调试”功能，固定为调试环境，不支持携带环境变量调试。

后续操作

创建完环境和环境变量后，您可以将API**发布到环境**，以便API调用者调用。

7 凭据管理

7.1 创建凭据并绑定 API

使用APP认证的API，需要在API网关中创建一个凭据，以生成凭据ID和密钥对（Key、Secret）。将创建的凭据绑定API后，才可以使用APP认证调用API。客户端（API调用者）在调用API过程中，把密钥对替换SDK中的密钥对，API网关服务根据密钥对进行身份核对，完成鉴权。关于使用APP认证的方法，具体请参考《API网关开发指南》。

说明

- 使用无认证/IAM认证的API，无需创建凭据。
- 每个实例最多创建50个凭据。

创建凭据

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击“创建凭据”，填写凭据信息。

表 7-1 凭据信息

信息项	描述
凭据名称	凭据的名称。
描述	对凭据的介绍。

说明

支持AppKey（Key）和AppSecret（Secret）自定义配置。AppKey是身份标识，需要保证全局唯一。如果没有特殊需求，不建议使用“自定义配置”，系统会默认生成全局标识，可在凭据详情中查看。

步骤5 单击“确定”，创建凭据。

- 创建凭据成功后，在凭据管理页面显示新建凭据和凭据ID。
- 单击*凭据名称*，进入详情页面，查看key和Secret。

----结束

绑定 API

步骤1 在“凭据管理”页面，单击*凭据名称*，进入详情页面。

步骤2 在“关联API”区域，单击“绑定API”。

步骤3 选择授权环境、API分组和API。

步骤4 单击“确定”。

如需解绑API，在API所在行单击“解绑”即可。

说明

一个凭据可以绑定多个APP认证的API，一个APP认证的API可以绑定多个凭据。

----结束

7.2 重置 Secret

Key唯一且不可重置，Secret支持重置，将Secret的值重新改变。重置完成后，原先的Secret将失效，绑定此凭据的API将无法调用，请更新SDK中的密钥对，并重新调用API。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击*凭据名称*，进入凭据详情页面。

步骤5 单击“重置Secret”。

步骤6 在弹窗中单击“确定”。

----结束

7.3 为简易认证绑定 AppCode

简易认证指调用API时，在HTTP请求头部消息增加一个参数X-Apig-AppCode（参数值填凭据详情中“AppCode”的值），而不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。

当使用APP认证，且开启了简易认证模式，API请求既可以选择使用Key和Secret做签名和校验，也可以选择使用AppCode进行简易认证。

说明

- 为了确保安全，简易认证仅支持HTTPS方式调用API，不支持HTTP。
- 每个凭据最多可创建5个AppCode。

生成 APPCode

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击*凭据名称*，进入凭据详情页面。

步骤5 在“AppCodes”区域，单击“添加AppCode”。

步骤6 在弹窗中配置AppCode，完成后单击“确定”。

表 7-2 配置 AppCode

信息项	描述
生成方式	选择AppCode的生成方式。 ● 自动生成：由系统随机生成AppCode。 ● 手动输入：自定义AppCode。
AppCode	仅手动输入方式需要填写AppCode的值。

----结束

使用 AppCode 进行 API 请求的简易认证

步骤1 在创建API时，选择“APP认证”并且开启“支持简易认证”。

说明

如果您修改已有API为简易认证，需要在修改完成后，将API重新发布，使简易认证模式生效。

步骤2 将支持简易认证的API绑定到已创建的凭据。

步骤3 发送请求时，增加请求头部参数“X-Apig-AppCode”，省略请求签名相关信息。

以Curl方式为例，增加头部参数名称：X-Apig-AppCode，参数值填已生成的AppCode。

```
curl -X GET "https://api.exampledemo.com/testapi" -H "content-type: application/json"  -H "host: api.exampledemo.com" -H "X-Apig-AppCode: xhrJVJKABSOxc7d**********FZL4gSHEXkCMQC"
```

----结束

7.4 绑定凭据配额策略

凭据配额策略用于限制客户端（API调用者）在某个时间周期内的API调用次数，支持自定义重置时间。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击*凭据名称*，进入凭据详情页面。

步骤5 在“凭据配额策略”区域，单击“绑定”。

步骤6 在弹窗中选择已有策略或单击“创建新策略”。

- 选择已有策略：单击“选择已有策略”后，选择策略。
- 创建新策略：请参考表7-3所示配置策略。

表 7-3 配置凭据配额策略

信息项	描述
策略名称	填写客户端配额策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写配额策略名称，方便您快速识别和查找。
首次生效时间点	设置配额策略的生效起始时间点。例如，时长为1小时，首次生效时间点为2020/08/08 05:05:00，则表示客户端配额策略从2020/08/08 05:05:00开始生效，每个小时的05分开始到下一个小时的05分之间为一个单位时间，即05:05:00-06:05:00为一个单位时间，以此类推。
时长	填写配额限制的时长，单位可选择“秒”、“分”、“时”和“天”。需与“API访问限制”配合使用，表示单位时间内客户端可调用API的总次数上限。
API访问限制	填写客户端可调用API的次数上限，与“时长”配合使用。
描述	填写客户端配额策略的描述信息。

步骤7 策略配置完成后，单击“确定”。

----结束

7.5 绑定访问控制策略

绑定访问控制策略可控制访问API的客户端（API调用者）IP地址，保护后端服务。您可以为客户端设置访问控制策略，允许/禁止某个IP地址的客户端访问API。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击*凭据名称*，进入凭据详情页面。

步骤5 在“访问控制策略”区域，单击“绑定”。

步骤6 在弹窗中配置策略信息。

表 7-4 绑定访问控制策略

信息项	描述
动作	选择访问控制的动作。 ● 允许：表示仅允许指定IP地址的客户端调用API。 ● 禁止：表示禁止指定IP地址的客户端调用API。
IP地址	单击“增加IP地址”，添加允许或禁止调用API的客户端IP地址或IP地址段。

步骤7 策略配置完成后，单击“确定”。

----结束

8 监控分析

8.1 API 监控

8.1.1 支持的监控指标

功能说明

本节定义了API网关服务上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供管理控制台来检索API网关服务产生的监控指标和告警信息。

命名空间

SYS.APIC

API 网关监控指标

表 8-1 API 网关监控指标说明

指标ID	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
requests	接口调用次数	统计测量api接口被调用的次数。	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
error_4xx	4xx异常次数	统计测量api接口返回4xx错误的次数。	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟

指标ID	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
error_5xx	5xx异常次数	统计测量api接口返回5xx错误的次数	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
throttled_calls	被流控的调用次数	统计测量api被流控的调用次数	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
avg_latency	平均延迟毫秒数	统计测量api接口平均响应延时时间	≥0 单位：毫秒	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
max_latency	最大延迟毫秒数	统计测量api接口最大响应延时时间	≥0 单位：毫秒	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
req_count	接口调用次数	该指标用于统计测量api接口调用次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_2xx	2xx调用次数	该指标用于统计测量api接口调用2xx的次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_4xx	4xx异常次数	该指标用于统计测量api接口返回4xx错误的次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_5xx	5xx异常次数	该指标用于统计测量api接口返回5xx错误的次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_error	异常次数	该指标用于统计测量api接口总的错误次数	≥0	测量对象：单个API 测量维度：api_id	1分钟

指标ID	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
avg_latency	平均延迟毫秒数	该指标用于统计测量api接口平均响应延时时间	≥0 单位：毫秒	测量对象：单个API 测量维度：api_id	1分钟
max_latency	最大延迟毫秒数	该指标用于统计测量api接口最大响应延时时间	≥0 单位：毫秒	测量对象：单个API 测量维度：api_id	1分钟
input_throughput	流入流量	该指标用于统计测量api接口请求流量	≥0 单位：Byte/KB/MB/GB	测量对象：单个API 测量维度：api_id	1分钟
output_throughput	流出流量	该指标用于统计测量api接口返回流量	≥0 单位：Byte/KB/MB/GB	测量对象：单个API 测量维度：api_id	1分钟

维度

表 8-2 API 网关监控指标测量维度

Key	Value
instance_id	专享版API网关
instance_id,api_id	API

8.1.2 创建告警规则

操作场景

通过创建告警规则，您可自定义监控目标与通知策略，及时了解API网关服务运行状况，从而起到预警作用。

告警规则包括告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数。

前提条件

API已被调用。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 在“API运行”页面的“监控视图”区域，单击“查看更多监控”，返回“云服务监控”界面，参考《云监控服务用户指南》的“创建告警规则”章节为API网关创建告警规则。

----结束

8.1.3 查看监控指标

云监控对API网关的运行状态进行日常监控，可以通过控制台直观的查看API网关各项监控指标。

查看单个 API 的监控指标

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*分组名称*。

步骤5 在“API运行”页面左侧选择API。

步骤6 在“监控视图”区域，查看API的各项监控指标。

步骤7 单击“查看更多监控”，查看更多监控数据。

说明

监控数据保留周期为两天，如果需要长时间保留，需要配置OBS桶，将监控数据保存至OBS桶中。

----结束

查看 API 分组的监控指标

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“监控分析 > API监控”。

步骤4 选择待查看的API分组，查看各项监控指标。

----结束

8.2 日志分析

快速获取并分析实例API的调用日志。

前提条件

已调用API。

操作步骤

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“监控分析 > 日志分析”。

步骤4 单击“配置访问日志”，将“启动日志记录”修改为  ，即启用日志记录能力。

步骤5 “日志组”和“日志流”设置请参见《云日志服务用户指南》的“日志管理”章节，完成后单击“确定”。

步骤6 查看日志分析可单击页面右上角“日志字段说明”，根据日志字段说明分析日志。

步骤7 如需导出日志，具体步骤请参见《云日志服务用户指南》的“日志转储”章节。

访问日志的字段采用空格作为分隔符，按照顺序，每个字段的含义如下：

表 8-3 日志字段说明

序号	字段	说明
1	remote_addr	客户端地址
2	request_id	请求ID
3	api_id	API ID
4	user_id	当使用IAM认证访问时，请求方提供的项目ID
5	app_id	当使用APP认证访问时，请求方提供的APP ID
6	time_local	请求时间
7	request_time	请求延迟
8	request_method	HTTP请求方法
9	host	请求域名
10	router_uri	请求URI
11	server_protocol	请求协议
12	status	响应状态码
13	bytes_sent	响应大小（单位：字节，包含状态行、响应头、响应体）
14	request_length	请求长度（单位：字节，包含起始行、请求头、请求体）

序号	字段	说明
15	http_user_agent	用户代理标识
16	http_x_forwarded_for	X-Forwarded-For头
17	upstream_addr	请求的后端地址
18	upstream_uri	请求后端的URI
19	upstream_status	后端响应状态码
20	upstream_connect_time	与后端建立连接所用时间
21	upstream_header_time	从开始与后端建立连接到从后端获取到首字节所用时间
22	upstream_response_time	从开始与后端建立连接到从后端获取到最后一个字节所用时间
23	region_id	云服务区ID
24	all_upstream_response_time	从开始与后端建立连接到从后端获取到最后一个字节所用时间，单位秒。发生重试时，为所用时间总和。
25	errorType	API请求的错误类型。 ● 0：非流控错误。 ● 1：流控错误。
26	auth_type	API认证类型。
27	access_model1	认证模式1。
28	access_model2	认证模式2，开启双重认证时，为自定义认证编号。
29	inner_time	apig的内部处理时长，单位秒。
30	proxy_protocol_vni	VPC终端节点的虚拟网络标识。
31	proxy_protocol_vpce_id	VPC终端节点的ID。
32	proxy_protocol_addr	客户端源IP地址。
33	body_bytes_sent	API请求的Body体大小，单位字节。
34	api_name	API名称。
35	app_name	当使用APP认证访问时，请求方使用的APP名称。
36	provider_app_id	API所属的APP ID。
37	provider_app_name	API所属的APP名称。
38	custom_data_log1	用户自定义日志字段值1。

序号	字段	说明
39	custom_data_log2	用户自定义日志字段值2。
40	custom_data_log3	用户自定义日志字段值3。
41	custom_data_log4	用户自定义日志字段值4。
42	custom_data_log5	用户自定义日志字段值5。
43	custom_data_log6	用户自定义日志字段值6。
44	custom_data_log7	用户自定义日志字段值7。
45	custom_data_log8	用户自定义日志字段值8。
46	custom_data_log9	用户自定义日志字段值9。
47	custom_data_log10	用户自定义日志字段值10。
48	response_source	请求响应来源。 ● local：APIG。 ● remote：后端服务。

----结束

9 实例管理

9.1 购买实例

本小节指导您顺利创建实例，实例创建完成后，才能创建API并对外提供服务。

购买的约束说明

创建实例存在一些约束，当您登录后无法创建实例，或者创建失败，请参考以下约束说明进行检查，并解除限制。

- 实例配额

  同一项目ID下，一个主帐号默认只能创建5个实例。如果您需要创建更多实例，可提交工单，申请修改配额。

- 用户权限

  如果您使用系统角色相关权限，需要同时拥有“APIG Administrator”和“VPC Administrator”权限才能创建实例。

  如果您使用系统策略，则拥有“APIG FullAccess”即可。

  如果使用自定义策略，请参考对用户组授权。

- 子网中可用私有地址数量

  API网关专享实例的基础版、专业版、企业版，以及铂金版分别需要3、5、6、7个私有地址。请确保您选择的子网段有足够多的私有地址可用，私有地址可在虚拟私有云服务的控制台查询。

网络环境准备

- 负载

  虚拟私有云。实例需要配置虚拟私有云（负载），在同一负载中的资源（如ECS），可以使用实例的私有地址调用API。

  在创建实例时，建议配置和您其他关联业务相同负载，确保网络安全的同时，方便网络配置。

  说明

  创建实例后，不支持修改虚拟私有云（负载）。

- 弹性公网IP

  实例的API如果要允许外部调用，则需要创建一个弹性公网IP，并与实例绑定，作为实例的公网入口。

  说明

  如果API的后端服务部署在公网，还需要有公网出口访问权限，这由API网关统一规划，不需要单独创建弹性公网IP。

- 安全组

  安全组类似防火墙，控制谁能访问实例的指定端口，以及控制实例的通信数据流向指定的目的地址。安全组入方向规则建议按需开放地址与端口，这样可以保护实例的网络安全。

  实例绑定的安全组有如下要求：

  - 入方向：如果需要从公网调用API，或从其他安全组内资源调用API，则需要为实例绑定的安全组的入方向放开**80**（HTTP）、**443**（HTTPS）两个端口。
  - 出方向：如果后端服务部署在公网，或者其他安全组内，则需要为实例绑定的安全组的出方向放开后端服务地址与API调用端口。
  - 如果API的前后端服务与实例绑定了相同的安全组、相同的虚拟私有云，则无需专门为实例开放上述端口。

操作步骤

步骤1 登录API网关控制台。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 单击“购买实例”。

表 9-1 API 网关实例参数说明

信息项	描述
区域	指APIG实例部署的区域，建议和您其他的业务部署在相同区域，这样不同的业务可以在负载内以子网方式通信，节省公网带宽成本，降低网络延时。
可用区	指同一区域内电力、网络等资源物理隔离的地理区域，一般为互相独立的机房。 APIG实例支持同时选择多个可用区，进行跨可用区部署，提升实例高可用性。
实例名称	实例的名称，根据规划自定义。
实例规格	当前开放基础版、专业版、企业版、铂金版实例。不同实例规格，对API请求的并发支持能力不同，具体请参考产品介绍的产品规格差异章节。
可维护时间窗	指允许云服务技术支持对实例进行维护的时间段。如果有维护需要，技术支持会提前与您沟通确认。 建议选择业务量较少的时间段。

信息项	描述
企业项目	使用企业用户登录时，可选择实例所属企业项目。 有关企业项目的资源使用、迁移以及用户权限等，请参考《企业管理用户指南》。
公网入口	指允许外部服务通过弹性IP地址，调用实例创建的API。开启“公网入口”，需要绑定一个“弹性IP地址”。 **说明** ● 您需要使用独立域名/调试域名访问，使用调试域名访问时存在单日访问次数限制。可在创建API分组后，为分组绑定独立域名，独立域名需要解析到实例的弹性IP地址。 例如您有一个API，请求协议为HTTPS，Path为/apidemo，开启了公网访问，并为分组绑定了独立域名后，可使用https://{domain}/apidemo这个URL访问您的API。其中，{domain}表示已绑定到分组的独立域名，目标端口443可默认缺省。
公网出口	指允许实例API的后端服务部署在外部网络，APIG为实例开启公网出口。您可以根据业务预估设置合适的“出公网带宽”，出公网带宽费用按小时计算，以弹性IP服务的价格为准。
网络	指为实例绑定到一个虚拟私有云，并为其分配子网。 在相同虚拟私有云中的云服务资源（如ECS），可以使用APIG实例的私有地址调用API。 建议将实例和您的其他关联业务配置一个相同的虚拟私有云，确保网络安全的同时，方便网络配置。
安全组	安全组用于设置端口访问规则，定义哪些端口允许被外部访问，以及允许访问外部哪些地址与端口。 例如，后端服务部署在外部网络，则需要设置相应的安全组规则，允许访问后端服务地址与API调用端口。 **说明** 如果开启公网入口，安全组入方向需要放开80（HTTP）和443（HTTPS）端口的访问权限。
描述	实例的描述信息。

步骤4 单击“立即购买”，进入实例规格确认页面。

步骤5 规格确认无误后，开始创建实例，界面显示创建进度。

----结束

后续操作说明

实例创建成功后，您可以开始创建和管理您的API。进入实例控制台后，概览界面展现实例信息、网络配置、配置参数等信息。

其中，实例名称、描述、时间窗、安全组，以及弹性IP地址等可以修改。

如果您要删除实例，请确认无业务影响后删除实例即可。

9.2 查看或编辑实例信息

实例创建完成后，可在控制台查看和编辑实例的配置信息。

操作步骤

步骤1 登录API网关控制台。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在待查看或编辑的实例上，单击“查看控制台”或*实例名称*。

步骤4 在“实例信息”页签，查看或编辑实例的配置信息。

表 9-2 实例信息

可编辑项	说明
基本信息	实例的基本信息，包括实例名称、实例ID、实例规格、可用区、描述、企业项目和时间窗。 ● 用户可以根据实际需要修改“实例名称”、“描述”等。 ● 用户可以单击“实例ID”右侧的 复制实例ID信息。
网络配置	● 虚拟私有云 实例所关联的VPC，用户可以单击VPC名称跳转查看VPC的具体配置信息。 ● 子网 实例所关联的子网，用户可以单击子网名称跳转查看子网的具体配置信息。 ● 安全组 实例所关联的安全组，用户可以单击安全组名称跳转查看安全组的具体配置信息，也可以单击 ，绑定新的安全组。
入口地址	● 虚拟私有云访问地址 ● 弹性IP地址 实例绑定的弹性IP地址。 – 如果实例未绑定弹性IP地址，您可以单击地址右侧的“立即启用”，绑定弹性IP地址。 – 如果实例已绑定弹性IP地址，您可以单击地址右侧的 复制地址信息。 – 如果实例已绑定弹性IP地址，您可以编辑公网带宽。公网带宽费用按小时计算，以弹性公网IP服务的价格为准。 – 如果实例已绑定弹性IP地址，您可以单击地址右侧的“解绑EIP”，解绑弹性IP地址。

可编辑项	说明
出口地址	指允许实例API的后端服务部署在外部网络，API网关为实例开启公网出口。公网出口可随时关闭或开启。
路由	配置私有网段。实例创建完成后，默认能够与创建时指定的VPC子网网段进行互通，如果有额外的私有网段需要与实例互通，可通过该配置项进行路由配置。 如果本地数据中心的子网不在以下三个大子网段内，暂时不支持配置本地路由：10.0.0.0/8-24、172.16.0.0/12-24、192.168.0.0/16-24。

----结束

9.3 配置参数

配置参数提供了实例内组件的公共参数配置，通过修改配置参数，可以调整组件的相关功能。

约束与限制

修改实例配置参数会引起APIG业务中断，建议在无业务运行或业务低峰时修改配置参数。

操作步骤

步骤1 登录API网关控制台。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在待配置参数的实例上，单击“查看控制台”或*实例名称*。

步骤4 单击“配置参数”页签，找到您需要调整的配置项并进行修改。不同的实例规格展示的配置参数会存在不同，具体以界面为准。

表 9-3 实例配置参数说明

信息项	描述
ratelimit_api_limits	API全局默认流控值。API未绑定流控策略时，执行此默认流控；API绑定流控策略时，则执行绑定的流控策略。流控策略的API流量限制值不能超过API全局默认流控值。
request_body_size	API请求中允许携带的Body大小上限。
backend_timeout	后端响应超时时间上限，可修改范围为1ms~600000ms。

信息项	描述
app_token	app_token认证方式开关。启用后，可在API请求中使用获取的access_token进行API的调用认证。 ● app_token_expire_time：access_token的有效时间，在access_token到期前，需要获取新的access_token。 ● refresh_token_expire_time：refresh_token的有效时间。refresh_token用于获取新的access_token。 ● app_token_uri：获取access_token的uri。 ● app_token_key：access_token的加密key。
app_basic	app_basic认证方式开关。启用后，在API请求中添加Header参数“Authorization”，参数值为"Basic"+base64(*appkey:appsecret*)，其中appkey和appsecret分别为凭据的Key和Secret（或客户端的AppKey和AppSecret）。
app_secret	app_secret认证方式开关。启用后，可在API请求中添加“X-HW-ID”和“X-HW-AppKey”参数，携带凭据的Key和Secret（或客户端的AppKey和AppSecret）进行API的调用认证。 使用app_secret认证时，需同时关闭app_api_key认证方式。
app_route	支持IP访问开关。启用后，非DEFAULT分组下的API可以使用IP地址调用。
backend_client_certificate	后端双向认证开关。启用后，创建API配置后端服务时，可配置后端双向认证。
ssl_ciphers	支持配置的https加密套件，可根据需要选择开启的加密套件。
real_ip_from_xff	是否使用X-Forwarded-For头中的IP作为ACL、流控的判断依据。 xff_index：X-Forwarded-For头中IP的排序序号，值允许为正数、负数、0。 ● xff_index值为0或正数时，获取X-Forwarded-For头中对应索引的IP。 ● xff_index值为负数时，按倒序方式从X-Forwarded-For头中获取IP。 例如到达API网关的X-Forwarded-For头中依次有IP1，IP2，IP3三个IP地址，xff_index取0时获取IP1，xff_index取1时获取IP2，xff_index取-1时获取IP3，xff_index取-2时获取IP2。
vpc_name_modifiable	负载通道名称是否可修改。 **须知** 负载通道名称可修改时，当前实例的负载通道无法通过项目级负载通道管理接口操作。

----结束

10 SDK

API网关开放的API，安全认证方式可选IAM认证、APP认证、自定义认证或无认证。四者的区别以及如何选择，请参考《API网关开发指南》中关于“如何选择认证方式”的介绍。本章节主要提供APP认证的SDK下载以及文档。

操作场景

API使用APP认证时，请根据需要下载SDK包和文档，参考文档完成API的调用。

操作步骤

步骤1 **登录API网关控制台**。

步骤2 在左侧导航栏选择“帮助中心”。

步骤3 单击“SDK使用指引”页签。

步骤4 在待下载的语言中，单击“下载SDK”，下载SDK包（SDK主要包含SDK代码和示例代码，不同语言SDK包不同）。

如需查看文档，请单击“SDK文档”。

----结束

11 调用已发布的 API

11.1 调用 API

获取 API 及文档

在调用API前，您需要向API提供者获取API的调用信息，包括访问域名、请求协议、请求方法、请求路径以及请求参数。

获取API：通过线下传递（如企业内部或者企业间合作）。

获取文档：如果API为云服务官方提供的服务，还可以在帮助中心获取参考文档。

根据API使用的安全认证方式，还要获取相关的请求认证信息：

- **APP认证**：
  - 签名认证：向API提供者获取该API所授权凭据的Key和Secret（或客户端的AppKey和AppSecret），以及用于调用API的SDK。
  - 简易认证：向API提供者获取该API所在凭据的AppCode。
  - 其他认证：向API提供者获取该API所授权凭据的Key和Secret（或客户端的AppKey和AppSecret）。
- **IAM认证**：通过云服务平台的帐号凭证（帐号和密码获取Token或者AK/SK）进行认证。如果使用AK/SK进行认证，还需要向API提供者获取用于调用API的SDK。
- **自定义认证**：向API提供者获取请求参数中要携带的自定义认证信息。
- **无认证**：无需认证信息。

调用 API

说明

本章节仅提供请求地址和认证参数的配置指导，客户端的其他参数配置需要用户自行调整，如超时配置、SSL配置等。如果客户端参数配置错误会导致业务受损，建议参考业界标准进行配置。

步骤1 配置请求地址相关参数。

API调用场景	API请求参数配置
使用域名调用API	使用服务分配的调试域名或服务绑定的域名调用API，无需另外配置。
使用IP调用DEFAULT分组的API	API允许使用IP地址调用DEFAULT分组下的API，无需另外配置。
使用IP调用非DEFAULT分组的API	● 使用IP地址直接调用非DEFAULT分组下的APP认证的API： 1. 将实例的**配置参数**“app_route”和“app_secret”设置为“on”。开启“app_route”之后，同一凭据不能授权给相同请求路径和方法的API。 2. 在请求消息中添加Header参数“X-HW-ID”和“X-HW-APPKEY”，参数值为API所授权凭据的Key和Secret或客户端的AppKey和AppSecret。 ● 使用IP地址直接调用非DEFAULT分组下的非APP认证的API，需要在请求消息中添加Header参数“host”。

步骤2 配置认证参数。

API认证方式	API请求参数配置
APP认证（签名认证）	使用获取的SDK对API请求进行签名，具体请参考《API网关开发指南》的“使用APP认证调用API”章节。
APP认证（简易认证）	在API请求中添加Header参数“X-Apig-AppCode”，参数值为**获取API及文档**中获取到的AppCode。具体请参考**快速入门**。
APP认证（app_secret认证）	● 实例的**配置参数**“app_secret”已设置为“on”，开启app_secret认证。 ● 在API请求中添加Header参数“X-HW-ID”，参数值为API所授权的Key或客户端的AppKey。 ● 在API请求中添加Header参数“X-HW-AppKey”，参数值为**获取API及文档**中获取到的Secret或AppSecret。
APP认证（app_basic认证）	● 实例的**配置参数**“app_basic”已设置为“on”，开启app_basic认证。 ● 在API请求中添加Header参数“Authorization”，参数值为"Basic"+base64(appkey+":"+appsecret)，其中appkey和appsecret分别为**获取API及文档**中获取到的Key和Secret（或AppKey和AppSecret）。
IAM认证（Token认证）	先获取云服务平台的认证Token，然后在API请求中携带Token进行认证，具体请参考《API网关开发指南》的“Token认证”章节。
IAM认证（AK/SK认证）	调用API时，使用获取的SDK对API请求进行签名，具体请参考《API网关开发指南》的“AK/SK认证”章节。
自定义认证	在API请求参数中携带认证信息进行认证。

API认证方式	API请求参数配置
无认证	无需认证，可直接调用API。

----结束

11.2 响应消息头

调用API时，API网关增加如下响应消息头。

X-Apig-Mode: debug表示响应消息头增加API网关调试信息。

响应消息头	描述	说明
X-Request-Id	请求ID	所有合法请求，都会返回此参数
X-Apig-Latency	从API网关接收请求到后端返回消息头的用时	仅在请求消息头包含X-Apig-Mode: debug时，返回此参数
X-Apig-Upstream-Latency	从API网关请求后端到后端返回消息头的用时	仅在请求消息头包含X-Apig-Mode: debug，且后端服务类型不为Mock时，返回此参数
X-Apig-RateLimit-api	API流量控制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了API流量控制时，返回此参数
X-Apig-RateLimit-user	用户流量限制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了用户流量限制时，返回此参数
X-Apig-RateLimit-app	凭据流量限制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了凭据流量限制时，返回此参数
X-Apig-RateLimit-ip	源IP流量限制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了源IP流量限制时，返回此参数
X-Apig-RateLimit-api-allenv	API默认流控信息 示例：remain:199,limit:200,time:1 second	仅在请求消息头包含X-Apig-Mode: debug时，返回此参数

11.3 错误码

当调用API时，可能遇到下表中的错误码。如果遇到“APIGW”开头的错误码，请参见《API签名指南》中的“错误码”进行处理。

说明

- 通过APIG接口管理API，发生错误时，产生的错误码请参考《API网关接口参考》的“错误码”章节。
- 使用APIG错误码时，请以错误码（如APIG.0101）为准，错误信息并非固定不变，有时会对错误信息进行优化修改。

表 11-1 错误码

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0101	The API does not exist or has not been published in the environment.	404	API不存在或未发布到环境	检查调用API所使用的域名、请求方法、路径和创建的API是否一致；检查API是否发布，如果发布到非生产环境，检查请求X-Stage头是否为发布的环境名；检查调用API使用的域名是否已经绑定到API所在的分组
APIG.0101	The API does not exist.	404	API请求方法不存在	检查API请求方法是否与API定义的方法相同
APIG.0103	The backend does not exist.	500	无法找到后端	联系技术支持
APIG.0104	The plug-ins do not exist.	500	无法找到插件配置	联系技术支持
APIG.0105	The backend configurations do not exist.	500	无法找到后端配置	联系技术支持
APIG.0106	Orchestration error.	400	编排错误	检查API配置的前后端参数是否合理
APIG.0201	API request error.	400	请求格式不合法	使用合法的请求
APIG.0201	Request entity too large.	413	请求body过大（大于12M）	减小请求body大小
APIG.0201	Request URI too large.	414	请求URI过大（大于32K）	减小请求URI大小

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0201	Request headers too large.	494	请求头过大（单个请求头大于32K或所有请求头总长度大于128K）	减小请求头大小
APIG.0201	Backend unavailable.	502	后端不可用	检查API配置的后端地址是否可用
APIG.0201	Backend timeout.	504	后端超时	增大超时时间或缩小后端的处理时间
APIG.0201	An unexpected error occurred	500	内部错误	联系技术支持
APIG.0202	Backend unavailable	502	后端不可用	检查API配置的后端请求协议是否与后端服务请求协议一致
APIG.0204	SSL protocol is not supported: TLSv1.1	400	SSL协议版本不支持	使用支持的SSL协议版本
APIG.0301	Incorrect IAM authentication information.	401	IAM认证信息错误	检查token是否正确
APIG.0302	The IAM user is not authorized to access the API.	403	IAM用户不允许访问API	检查用户是否被黑白名单限制
APIG.0303	Incorrect app authentication information.	401	APP认证信息错误	检查请求的方法、路径、查询参数、请求体和签名使用的方法、路径、查询参数、请求体是否一致；检查客户端机器时间是否正确。请参考《开发指南》的“使用APP认证调用API”章节检查签名代码的问题
APIG.0304	The app is not authorized to access the API.	403	APP不允许访问API	检查APP是否授权访问API
APIG.0305	Incorrect authentication information.	401	认证信息错误	检查认证信息是否正确

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0306	API access denied.	403	不允许访问API	检查是否授权访问API
APIG.0307	The token must be updated.	401	token需要更新	重新从IAM获取token
APIG.0308	The throttling threshold has been reached.	429	超出流控值限制	等待流控刷新后访问。如果触发调试域名的单日请求数上限，请绑定独立域名
APIG.0310	The project is unavailable.	403	project不可使用	使用其他project访问
APIG.0311	Incorrect debugging authentication information.	401	调试认证信息错误	联系技术支持
APIG.0401	Unknown client IP address.	403	无法识别客户端IP地址	联系技术支持
APIG.0402	The IP address is not authorized to access the API.	403	IP地址不允许访问	检查IP地址是否被黑白名单限制
APIG.0404	Access to the backend IP address has been denied.	403	后端IP不允许访问	后端IP地址或后端域名对应的IP地址不允许访问
APIG.0502	The app has been frozen.	405	APP被冻结	余额不足
APIG.0601	Internal server error.	500	内部错误	联系技术支持
APIG.0602	Bad request.	400	非法请求	检查请求是否合法
APIG.0605	Domain name resolution failed.	500	域名解析失败	检查域名拼写，以及域名是否绑定了正确的后端地址
APIG.0606	Failed to load the API configurations.	500	未加载API配置	联系技术支持
APIG.0607	The following protocol is supported: {xxx}	400	协议不被允许，允许的协议是*xxx*。 注意：xxx以实际响应中的内容为准。	改用支持的协议（HTTP/HTTPS）访问

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0608	Failed to obtain the admin token.	500	无法获取管理帐户	联系技术支持
APIG.0609	The VPC backend does not exist.	500	找不到负载后端	联系技术支持
APIG.0610	No backend available.	502	没有可连接的后端	检查所有后端是否可用，如调用信息与实际配置是否一致
APIG.0611	The backend port does not exist.	500	后端端口未找到	联系技术支持
APIG.0612	An API cannot call itself.	500	API调用自身	修改API后端配置，递归调用层数不能超过10层
APIG.0613	The IAM service is currently unavailable.	503	IAM服务暂时不可用	联系技术支持
APIG.0705	Backend signature calculation failed.	500	计算后端签名失败	联系技术支持
APIG.0802	The IAM user is forbidden in the currently selected region	403	该IAM用户在当前region中被禁用	联系技术支持
APIG.1009	AppKey or AppSecret is invalid	400	AppKey或AppSecret不合法	检查请求的AppKey或AppSecret是否正确

12 权限管理

12.1 创建用户并授权使用 API 网关

如果您需要对您所拥有的API网关服务进行权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的云帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用API网关服务资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将API网关服务资源委托给更专业、高效的其他帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果云帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用API网关服务的功能。

本章节为您介绍对用户授权的方法，操作流程如图12-1所示。

前提条件

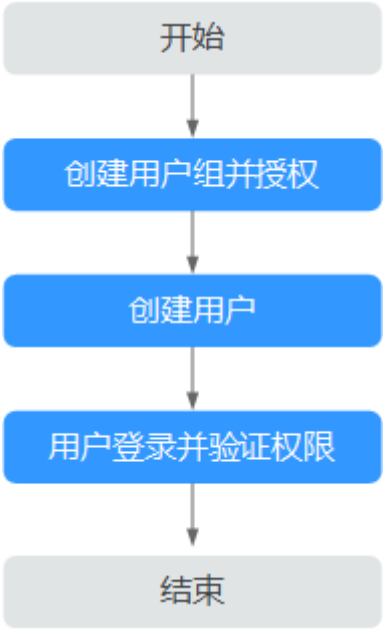
给用户组授权之前，请您了解用户组可以添加的表12-1，并结合实际需求进行选择。

表 12-1 API 网关的系统角色或策略

系统角色/策略名称	描述	类别	依赖关系
APIG Administrator	API网关服务的管理员权限。拥有该权限的用户可以使用API网关服务的所有功能。	系统角色	无。
APIG FullAccess	API网关服务所有权限。拥有该权限的用户可以使用API网关服务的所有功能。	系统策略	无。
APIG ReadOnly Access	API网关服务的只读访问权限。拥有该权限的用户只能查看API网关的各类信息。	系统策略	无。

示例流程

图 12-1 给用户授权 API 网关服务权限流程



1. 创建用户组并授权

   在IAM控制台创建用户组，并授予API网关服务的权限“APIG Administrator”或“APIG FullAccess”。

2. 创建用户并加入用户组

   在IAM控制台创建用户，并将其加入1中创建的用户组。

3. 用户登录并验证权限

   新创建的用户登录控制台，验证API网关服务的权限。

12.2 API 网关自定义策略

如果系统预置的API网关权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考《API网关接口参考》中的“权限策略和授权项”。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：《统一身份认证服务》中的“创建自定义策略”章节。本章为您介绍常用的API网关自定义策略样例。

API 网关自定义策略样例

- 示例1：授权用户创建API、调试API的权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                        apig:apis:create
                        apig:apis:debug
                    "
            ]
        }
    ]
}
```

- 示例2：拒绝用户创建API分组

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予APIG FullAccess的系统策略，但不希望用户拥有APIG FullAccess中定义的创建API分组权限，您可以创建一条拒绝创建API分组的自定义策略，然后同时将APIG FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以执行除创建API分组外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                        apig:apis:create
                        apig:apis:debug
                    "
            ]
        }
    ]
}
```

13 云审计服务支持的关键操作

13.1 云审计服务支持的 APIG 操作列表

开通云审计服务

如果您需要收集、记录或者查询API网关服务的操作日志，用于支撑安全分析、审计、问题定位等常见应用场景时，那么需要先开通云审计服务，具体请参见《云审计服务用户指南》的“开通云审计服务”章节。

云审计服务包含以下功能：

- 记录审计日志
- 审计日志查询
- 审计日志转储
- 事件文件加密
- 关键操作通知

查看关键操作列表

通过云审计服务，您可以记录与API网关相关的操作事件，便于日后的查询、审计和回溯。

表 13-1 云审计服务支持的 API Gateway 操作列表

操作名称	资源类型	事件名称
创建API分组	ApiGroup	createApiGroup
删除API分组	ApiGroup	deleteApiGroup
更新API分组	ApiGroup	updateApiGroup
绑定域名	ApiGroup	createDomainBinding
修改安全传输协议	ApiGroup	modifySecureTransmission

操作名称	资源类型	事件名称
解绑域名	ApiGroup	relieveDomainBinding
添加域名证书	ApiGroup	addDomainCertificate
删除域名证书	ApiGroup	deleteDomainCertificate
创建API	Api	createApi
删除API	Api	deleteApi
批量删除API	Api	batchDeleteApi
更新API	Api	updateApi
发布API	Api	publishApi
下线API	Api	offlineApi
批量发布/下线API	Api	batchPublishOrOfflineApi
切换API版本	Api	switchApiVersion
根据版本号下线API	Api	offlineApiByVersion
调试API	Api	debugApi
创建环境	Environment	createEnvironment
删除环境	Environment	deleteEnvironment
更新环境	Environment	updateEnvironment
创建环境变量	EnvVariable	createEnvVariable
更新环境变量	EnvVariable	updateEnvVariable
删除环境变量	EnvVariable	deleteEnvVariable
创建凭据	App	createApp
删除凭据	App	deleteApp
更新凭据	App	updateApp
重置签名密钥	App	resetAppSecret
客户端绑定API	AppAuth	grantAuth
客户端解绑API	AppAuth	relieveAuth
创建签名密钥	Signature	createSignature
删除签名密钥	Signature	deleteSignature
更新签名密钥	Signature	updateSignature
绑定签名密钥	SignatureBinding	createSignatureBinding
解绑签名密钥	SignatureBinding	relieveSignatureBinding

操作名称	资源类型	事件名称
创建访问控制	Acl	createAcl
删除访问控制	Acl	deleteAcl
批量删除访问控制	Acl	batchDeleteAcl
更新访问控制	Acl	updateAcl
增加流控黑名单	Acl	addAclValue
删除流控黑名单	Acl	deleteAclValue
API绑定访问控制	AclBinding	createAclBinding
API解绑访问控制	AclBinding	relieveAclBinding
批量解绑访问控制	AclBinding	batchRelieveAclBinding
创建流控	Throttle	createThrottle
删除流控	Throttle	deleteThrottle
批量删除流控	Throttle	batchDeleteThrottle
更新流控	Throttle	updateThrottle
绑定流控	ThrottleBinding	createThrottleBinding
解绑流控	ThrottleBinding	relieveThrottleBinding
批量解绑流控	ThrottleBinding	batchRelieveThrottleBinding
创建特殊流控	ThrottleSpecial	createSpecialThrottle
删除特殊流控	ThrottleSpecial	deleteSpecialThrottle
更新特殊流控	ThrottleSpecial	updateSpecialThrottle
创建负载通道	Vpc	createVpc
删除负载通道	Vpc	deleteVpc
更新负载通道	Vpc	updateVpc
增加负载通道成员	Vpc	addVpcMember
删除负载通道成员	Vpc	deleteVpcMember
导出单个API	Swagger	swaggerExportApi
批量导出API	Swagger	swaggerExportApiList
导出分组下所有API	Swagger	swaggerExportApiByGroup
导入API到新分组	Swagger	swaggerImportApiToNewGroup

操作名称	资源类型	事件名称
导入API到已有分组	Swagger	swaggerImportApiToExistGroup
导出全部自定义后端	Swagger	SwaggerExportLdApi
导入自定义后端	Swagger	SwaggerImportLdApi
创建自定义认证	Authorizer	createAuthorizer
删除自定义认证	Authorizer	deleteAuthorizer
更新自定义认证	Authorizer	updateAuthorizer
创建插件	Plugin	createPlugin
更新插件	Plugin	updatePlugin
删除插件	Plugin	deletePlugin
插件绑定API	Plugin	pluginAttachApi
解除绑定插件的API	Plugin	pluginDetachApi
API绑定插件	Plugin	apiAttachPlugin
解除绑定API的插件	Plugin	apiDetachPlugin

关闭云审计服务

如果需要关闭云审计服务，具体步骤请参见《云审计服务用户指南》的“删除追踪器”章节。

13.2 查看云审计日志

如果需要查看审计日志，具体步骤请参见《云审计服务用户指南》的“查看追踪事件”章节。

图 13-1 查看日志

14 常见问题

14.1 热门咨询

API 创建

- 不使用VPC通道（负载通道）时，后端服务地址可以是什么？
- 后端服务地址是否一定要配置为ECS的地址？
- 后端服务是否支持绑定私网ELB地址？
- 后端服务地址可以填写私有地址（子网IP）吗？
- API网关可以绑定内网域名吗？

API 调用

- API调用失败的可能原因有哪些？
- API调用返回错误码如何处理？
- "The API does not exist or has not been published in the environment."如何解决？
- No backend available，怎么解决？
- 后端服务调用失败“Backend unavailable”或超时“Backend timeout”原因分析

API 认证鉴权

- 是否支持HTTPS的双向认证？
- “无认证”方式的API该怎么鉴权与调用？

API 控制策略

- 是否支持对请求并发次数做自定义控制？
- API调用是否存在带宽限制
- 怎样给指定的用户开放API
- 配置了身份认证的API，如何在特殊场景下（如指定IP地址）允许不校验身份？

API 导入导出

- API导入失败是什么原因?
- swagger导入API的扩展字段有没有模板?

14.2 API 创建

14.2.1 无法创建 API 是什么原因?

API免费创建。如果被限制操作，可能原因为用户欠费。

14.2.2 API 的响应码如何定义?

响应信息由后端API服务（即API的提供者）定义，API网关只做透传。

14.2.3 使用 VPC 通道（负载通道），后端服务的主机端口怎么填写?

填写API后端服务的端口。

14.2.4 不使用 VPC 通道（负载通道）时，后端服务地址可以是什么?

可以是公网域名或者公网IP（支持云服务器的弹性IP地址）。

14.2.5 后端服务地址是否一定要配置为 ECS 的地址?

后端服务地址可以配置为ECS的弹性公网IP，也可以配置为您自己服务器的公网IP地址，还可以配置为域名。

14.2.6 后端服务是否支持绑定私网 ELB 地址?

- 专享版APIG支持绑定私网ELB地址。
- 如果是公网ELB地址，可直接使用。

14.2.7 后端服务地址可以填写私有地址（子网 IP）吗?

专享版：支持。实例所在同一个vpc子网内IP，或者通过专线打通的本地数据中心私有地址。

不支持专享版的网段：

- 0.0.0.0/8
- 10.0.0.0/8
- 100.125.0.0/16
- 127.0.0.0/8
- 169.254.0.0/16
- 172.16.0.0/12

- 192.0.0.0/24
- 192.0.2.0/24
- 192.88.99.0/24
- 192.168.0.0/16
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/4
- 240.0.0.0/4
- 255.255.255.255/32

14.2.8 API 网关是否支持多后端节点方案?

支持，通过VPC通道（负载通道）支持多后端节点，一个VPC通道中可以添加多个云服务器。

14.2.9 独立域名申请后还需要做什么?

独立域名完成注册、备案后，对于专享版，您需要将其A记录解析到实例的入口地址。解析成功后，即可使用。域名与API分组为多对一的关系，即一个分组最多能绑定5个独立域名，但一个域名只能解析到1个分组。

说明

若您使用的公网域名，需要在DNS服务公网解析内注册A记录（专享版）。

若您使用的内网域名，需要在DNS服务内网解析内注册A记录（专享版），还需要关联后端服务所属的VPC。

14.2.10 API 网关可以绑定内网域名吗?

对于专享版，可以配置内网域名，并将A记录解析到实例的入口地址。

14.2.11 为什么分组跨域配置失败?

1. 检查是否开启CORS。

   进入API详情，单击“编辑”，查看是否开启CORS。若没开启CORS，请开启。

2. 检查是否创建OPTIONS方式的API，每个分组只需创建一个OPTIONS方式的API。

   说明

   参数配置如下：

   所属分组：选择已开启CORS的API所在分组。

   请求方法：选择OPTIONS。

   请求协议：选择与已开启CORS的API相同的请求协议。

   请求路径：选择与已开启CORS的API相同的请求路径或者与已开启CORS的API匹配的请求路径。

   匹配模式：选择前缀匹配。

   安全认证：“无认证”模式安全级别低，所有用户均可访问，不推荐使用。

   支持跨域CORS：勾选。

14.3 API 调用

14.3.1 API 调用失败的可能原因有哪些?

网络问题

调用API失败的场景分为三种：同一VPC内调用失败、不同VPC之间调用失败、公网调用失败。

- VPC内调用API失败时，请检查域名是否和API自动分配的域名一致，如果域名错误，会导致调用API失败。
- 不同VPC之间调用API失败时，请检查两个VPC的网络是否互通。如果不通，可以通过创建VPC对等连接，将两个VPC的网络打通，实现跨VPC访问实例。

  关于创建和使用VPC对等连接，请参考《虚拟私有云用户指南》中的“对等连接”章节，或《API网关最佳实践》中的“API网关跨VPC开放后端服务”章节。
- 公网调用API失败时，可能的原因如下：
  - API没有绑定弹性公网IP（EIP），导致API缺少公网访问的有效地址，公网调用API失败。

    绑定EIP后重新调用即可，详细步骤请参考《API网关用户指南》中“购买实例”章节。
  - 入方向规则配置有误，导致公网调用API失败。

    配置入方向规则的详细步骤请参考《API网关用户指南》中“购买实例”章节。
  - 调用时未添加请求消息头“host:分组域名”，导致公网调用API失败。添加消息头后，重新调用即可。

域名问题

- 域名是否备案成功，且能正常解析。
- 域名是否绑定到正确的API分组。
- 子域名（调试域名）访问超过默认次数。API分组创建后，系统为分组自动分配一个内部测试用的子域名，此子域名唯一且不可更改，每天最多可以访问1000次。您可以通过添加独立域名来访问您开放的API。

发布问题

API是否已发布。如果修改过API，则需要重新发布；如果发布到非RELEASE环境，请求X-Stage头的值需要填写发布的环境名称。

API 认证鉴权

如果使用APP认证，App Key和Secret是否正确。

API 控制策略

- 访问控制策略是否设置正确。

- 是否超过了流量控制范围。系统默认的流控策略是单个API的访问不超过200次/秒，如果您未创建流控策略，API网关会执行默认流控策略。您可以在实例控制台“实例信息”页面中的“配置参数”页签下，通过修改“ratelimit_api_limits”参数来设置API的默认流控策略。

14.3.2 API 调用返回错误码如何处理?

如果您直接调用自己创建的API，参考错误码。

如果您使用接口管理您的API，参考《API网关接口参考》中的“错误码”章节。

14.3.3 API 调用报错“414 Request-URI Too Large”

可能原因：URL（包括请求参数）太长，建议将请求参数放在body体中传递。

14.3.4 "The API does not exist or has not been published in the environment."如何解决?

调用API网关中开放的API报错，请按以下顺序排查可能原因：

1. 调用API所使用的域名、请求方法、路径不正确。
   - 比如创建的API为POST方法，您使用了GET方法调用。
   - 比如访问的URL比API详情中的URL少一个“/”也会导致无法匹配上此API，例如http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test/和http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test会匹配上不同的API。
2. API没有发布。API创建后，需要发布到具体的环境后才能使用。具体操作请参考《API网关用户指南》中“发布API”章节。如果发布到非生产环境，检查请求“X-Stage”头是否为发布的环境名。
3. 域名解析不正确。如果API的域名、请求方法、路径正确，且已发布到环境，有可能是没有准确解析到您的API所在分组。请检查API所在的分组域名，例如您有多个API分组，每个分组有自己的独立域名，API调用时，使用了其他分组的独立域名。
4. 检查API是否使用OPTIONS跨域请求，如果使用OPTIONS跨域请求，请在API中开启CORS，并创建OPTIONS方式的API。具体操作请参考《API网关用户指南》中“开启跨域共享”章节。

14.3.5 No backend available，怎么解决?

- 检查后端服务是否可以访问，如果不能访问，请修改后端服务。
- 检查后端服务对应的ECS安全组配置，查看是否已开放您需要的端口。
- 检查VPC网络中的ACL配置，查看是否有相关ACL策略限制了API网关实例与后端服务所在子网的通信。
- 若使用VPC通道，检查VPC通道业务端口、健康检查端口、后端服务器添加是否均正常。

14.3.6 后端服务调用失败“Backend unavailable”或超时“Backend timeout”原因分析

以下原因可能导致后端服务调用失败或者超时，请逐一排查。

原因	解决方案
后端服务地址错误。	在编辑API中修改后端服务地址。 如果是域名，请确认域名能正确解析到后端服务IP地址。
后端超时时间设置不合理。 当后端服务没有在设置的后端超时时间内返回时，API网关提示后端服务调用失败。	在编辑API中增加后端超时时间。
如果“后端服务地址”在ECS（Elastic Cloud Server），ECS的安全组的出/入方向规则可能拦截了请求。	检查后端服务所在ECS的安全组，确保出/入方向端口规则和协议都设置正确。
请求协议配置错误，如后端服务为HTTP，在API网关配置为HTTPS。	创建的API与后端服务配置相同的协议。
API网关客户侧后端服务链接链路不通。	排查链接链路。

14.3.7 后端服务调用报错域名无法解析“Backend domain name resolution failed”

APIG实例所在的VPC完成了内网域名解析，后端服务调用仍报“域名无法解析”错误。

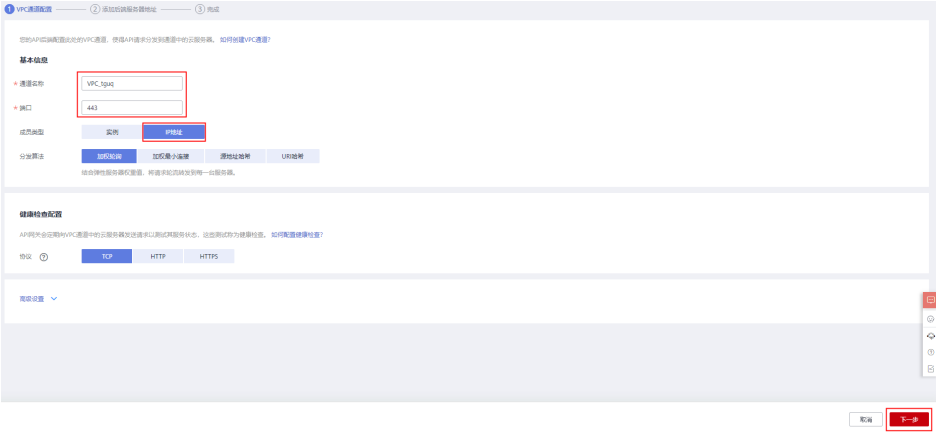
可能原因

APIG实例所在的VPC与用户后端服务所在的VPC存在网络隔离，内网域名解析仅在用户后端服务所在的VPC下能够解析。

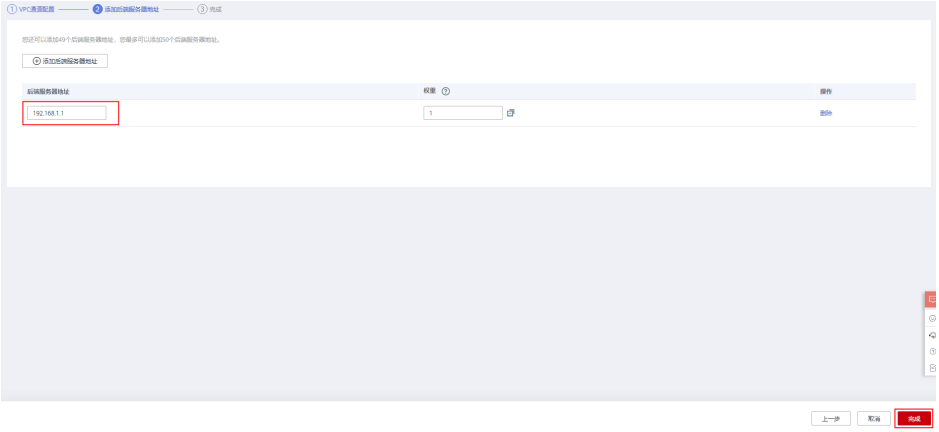
解决方法

- 方法一：在创建API时，使用公网域名配置“后端服务地址”。
- 方法二：在创建API时，不使用负载通道，使用用户后端服务IP配置“后端服务地址”，添加常量参数，在HEADER中添加Host：域名字段。

- 方法三：在创建API时，使用负载通道。
  a. 创建负载通道。



b. 添加用户后端服务地址。



c. 创建API时，使用负载通道，配置自定义头域。

14.3.8 修改后端服务的超时时间上限“backend_timeout”后未生效

问题描述

修改专享版APIG实例参数“backend_timeout”后未生效。

可能原因

在“定义后端服务”中，“后端超时(ms)”未修改。

解决方法

登录控制台，进入目标API详情，单击“编辑”，在“定义后端服务”中配置“后端超时(ms)”。

14.3.9 如何切换调用环境?

默认调用“发布”环境的API。如果您要调用其他环境的API，请添加请求消息头X-Stage，参数值填写环境名称。

14.3.10 调用请求包最大支持多少?

专享版：API每次最大可以转发Body体为12MB的请求包。请求body体超过12M时，根据业务需求，请在“实例概览”的配置参数中修改“request_body_size”参数。“request_body_size”表示API请求中允许携带的Body大小上限，支持修改范围1~9536 M。

14.3.11 使用 iOS 系统时，如何进行 APP 认证?

目前API网关为APP认证提供了Java、Python、C、PHP、Go等多种语言的SDK与demo，当您使用iOS系统（Objective-C语言）或者其他未包含在内的语言时，请参考“开发指南 > 使用APP认证调用API > APP认证工作原理”的指导进行APP认证。

14.3.12 新建一个 IAM 认证方式的 API，在配置入参时为什么无法配置 HEADER 位置的 x-auth-token?

x-auth-token在API网关内部已经被定义了，如果您再次创建此参数名，容易导致冲突。API网关console中已经限定您无法创建HEADER位置的x-auth-token，您只需在调用此API时，直接在header中增加x-auth-token和其值即可。

14.3.13 凭据问题汇总

Q：最多支持创建多少个凭据?

每个用户最多创建50个凭据。

Q：APP认证的API，怎样实现不同的第三方之间无法知道对方调用情况?

创建多个凭据，并绑定同一个API，分发给不同的第三方不一样的凭据。

Q：APP认证的API，有没有限制可以给多少个第三方使用?

没有限制。

Q：APP认证的API，是否需要自己创建凭据?

是，需要自行创建凭据，并绑定API。创建完成凭据后，系统自动生成AppKey和AppSecret，将AppKey和AppSecret给第三方，就可以直接调用此API了。

Q：APP认证的API，第三方怎么调用?

您需要把AppKey和AppSecret提供给第三方，然后第三方通过SDK调用。具体SDK的调用步骤请参见“开发指南 > 使用APP认证调用API”。

14.3.14 是否支持移动应用调用 API?

API支持被移动应用调用。使用APP认证时，将移动应用的AppKey和AppSecrect替换SDK中的AppKey和AppSecrect进行APP签名。

14.3.15 部署在 VPC 下的应用是否可以调用 API?

默认部署在VPC下的应用可以调用API。如果域名解析失败，则参考**配置内网DNS**，在当前终端节点上配置DNS服务器。配置完成后，部署在VPC下的应用可以调用API。

配置内网 DNS

配置DNS需要配置“/etc”目录下的**resolv.conf**文件，指定DNS服务器的IP地址。

内网DNS服务器的IP地址与您所位于的区域相关，您可通过《云解析服务DNS》的“常见问题”中提供的内网DNS地址获取内网DNS服务器的IP地址。

新增内网DNS服务器有两种方法。

- 方法一：修改虚拟私有云的子网信息。
- 方法二：编辑“/etc/resolv.conf”文件。

说明

方法二新增的内网DNS在弹性云服务器每次重启后会失效，需要重新进行配置。因此，建议使用方法一。

方法一：

您可以按如下步骤修改虚拟私有云的子网信息，将DNS服务器地址添加到弹性云服务器对应的子网中。

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 ，选择区域。

步骤3 在服务列表中，单击“计算 > 弹性云服务器”，进入弹性云服务器管理页面。

步骤4 单击待使用的弹性云服务器名称，进入弹性云服务器详情页面。

步骤5 在“网卡”页签，单击 ，查看弹性云服务器的子网名称。

步骤6 在弹性云服务器“基本信息”页面中，查看弹性云服务器的虚拟私有云名称。

步骤7 单击虚拟私有云名称，进入“网络控制台 > 虚拟私有云”页面。

步骤8 在左侧导航栏单击“子网”。

步骤9 找到步骤5中对应的子网，单击子网名称。

步骤10 修改该子网的“DNS服务器地址”，单击“确定”。

例如，将“DNS服务器地址”修改为“100.125.1.250”。

步骤11 重启弹性云服务器。查看“/etc/resolv.conf”文件的内容，确认其中包含待配置的DNS服务器地址，并且DNS服务器地址位于其他DNS服务器地址之前。

例如，如下图所示，DNS服务器地址为“100.125.1.250”。

```
# Generated by NetworkManager
search openstacklocal
nameserver 100.125.1.250
nameserver 114.114.115.115
```

说明

对虚拟私有云的子网信息的修改会影响所有使用该子网创建的弹性云服务器。

----结束

方法二

编辑“/etc/resolv.conf”文件，新增内网DNS服务器地址。

例如，您位于“region01”，则需要在“/etc/resolv.conf”文件中新增一个IP地址为“100.125.1.250”的内网DNS服务器。

说明

- 新增的DNS服务器地址必须位于原有的DNS服务器地址之前。
- 保存“/etc/resolv.conf”文件后，DNS配置操作立即生效。

14.3.16 如何实现 WebSocket 数据传输?

API网关支持WebSocket数据传输，在创建API时，请求协议中的HTTP相当于WebSocket的ws，HTTPS相当于WebSocket的wss。

14.3.17 API 调用是否支持长连接

API网关支持长连接，但注意适当使用，避免占用太多资源。

14.3.18 策略后端有多个时，怎么匹配和执行

当您的API配置了多个策略后端，API网关会按顺序进行匹配，匹配到其中一个立即执行API请求转发，不会进行后续的匹配。

当策略后端都没有匹配成功，则按照默认后端执行API请求的转发。

14.3.19 API 调用对请求的响应消息体限制

API调用对请求的响应消息体大小没有限制。

14.3.20 如何通过 APIG 访问公网后端服务

通过开启实例的公网入口访问，允许外部服务调用API。

如果您在调用API遇到网络问题，请参考**API调用失败的可能原因有哪些？**。

14.4 API 认证鉴权

14.4.1 是否支持 HTTPS 的双向认证?

专享版：支持。

- 后端双向认证。在创建API时，配置双向认证，在API网关和后端服务间启用双向认证。配置请参考**创建API**中的“双向认证”参数说明。

14.4.2 “无认证”方式的 API 该怎么鉴权与调用?

“无认证”即API网关对收到的调用请求不做身份认证，您只需要按照API提供者提供的接口说明，封装规范的HTTP请求，发送给API网关即可。

说明

无认证方式下，API网关把请求内容**透传**给后端服务。因此，如果您希望在API后端服务进行鉴权，可以使用“无认证”方式，API调用方传递鉴权所需字段给后端服务，由后端服务进行鉴权。

14.4.3 TLS 加密协议支持什么版本?

API网关支持TLS 1.1及TLS 1.2版本，暂不支持TLS 1.0或TLS 1.3。

14.4.4 API 签名认证能否自定义鉴权方式?

支持。请参考《API网关用户指南》的“自定义认证”章节。

14.4.5 安全认证签名的内容是否包括 Body 体

包括。除了几个必选的请求头部参数，Body体也是签名要素之一。例如有一个使用POST方法上传文件的API，那么在签名过程中，会取这个文件的hash值，参与生成签名信息。

关于签名的详细内容，可参考：《API网关开发指南》中的“APP认证工作原理”章节。

14.4.6 IAM 认证信息错误

IAM认证信息错误有：

- **Incorrect IAM authentication information: verify aksk signature fail**
- **Incorrect IAM authentication information: AK access failed to reach the limit,forbidden**
- **Incorrect IAM authentication information: decrypt token fail**
- **Incorrect IAM authentication information: Get secretKey failed**

Incorrect IAM authentication information: verify aksk signature fail

```
{
  "error_msg": "Incorrect IAM authentication information: verify aksk signature fail, ......
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

可能原因

签名认证算法使用有问题，客户端计算的签名结果与API网关计算的签名结果不同。

解决方法

步骤1 获取API网关计算的canonicalRequest。

从报错信息的body中获取“request_id”，通过“request_id”查找shubao节点的error.log（error.log在CLS上查看），在error.log中获取canonicalRequest。

```
2019/01/26 11:34:27 [error] 1211#0: *76 [lua] responses.lua:170: rewrite():
473a4370fbaf69e42f9da243eb8f8c52;app-1;Incorrect IAM authentication information: verify signature
fail;SDK-HMAC-SHA256 Access=071fe245-9cf6-4d75-822d-c29945a1e06a, SignedHeaders=host;x-sdk-date,
Signature=b2ef2cddcef89cbfe22974c988909c1a94b1ac54114c30b8fe083d34a259e0f5;canonicalRequest:GE
T
/app1/

host:test.com
x-sdk-date:20190126T033427Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855, client: 192.168.0.1, server:
shubao, request: "GET /app1 HTTP/1.1", host: "test.com"
```

步骤2 通过打印日志或调试中断的方式得到客户端计算的canonicalRequest，每种语言SDK中计算canonicalRequest的位置如下：

表 14-1 常见语言 SDK 中计算 canonicalRequest 的位置

语言	位置
java	libs/java-sdk-core-..*.jar中com.cloud.sdk.auth.signer.DefaultSigner.class中的sign函数。
c	signer.c中的sig_sign函数。
c++	signer.cpp中的Signer::createSignature函数。
c#	signer.cs中的Sign函数。
go	signer.go中的Sign函数。
JavaScript	signer.js中的Signer.prototype.Sign函数。
python	signer.py中的Sign函数。
php	signer.php中的Sign函数。

例如，在调试中断位置获取的cannonicalRequest。

```
POST
/app1/
```

```
host:test.com
x-sdk-date:20190126T033950Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

步骤3 比较步骤1和步骤2中的cannonicalRequest是否一致。

- 是，请检查appsecret或sk是否正确。（常见问题：appsecret或sk中多填了空格）
- 否。
  - 第1行不同：请求方法要保持一致。
  - 第2行不同：请求路径要保持一致。
  - 第3行不同：请求参数要保持一致。
  - 第4-5行不同：请求头信息，每行都要保持一致。
  - 第7行不同：请求头参数名个数要和请求头信息行数保持一致。
  - 第8行不同：请求body要保持一致。

表 14-2 比较 API 网关和客户端计算的 canonicalRequest

行数	参数	API网关	客户端
1	请求方法	GET	POST
2	请求路径	/app1/	/app1/
3	请求参数	空	空
4	请求头信息	host:test.com	host:test.com
5	请求头信息	x-sdk-date: 20190126T033427Z	x-sdk-date: 20190126T033950Z
6	空行	-	-
7	请求头参数名列表	host;x-sdk-date	host;x-sdk-date
8	请求body的hash值	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

----结束

Incorrect IAM authentication information: AK access failed to reach the limit,forbidden

```
{
  "error_msg": "Incorrect IAM authentication information: AK access failed to reach the limit,forbidden." ......
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

可能原因

- aksk签名计算错误。请参考**Incorrect IAM authentication information: verify aksk signature fail**解决方法。
- ak对应的sk不匹配。
- aksk频繁出现鉴权出错，连续错误5次以上，被锁定5分钟（5分钟内鉴权失败，误以为是异常的鉴权请求）。
- token鉴权时，token过期。

Incorrect IAM authentication information: decrypt token fail

```
{
  "error_msg": "Incorrect IAM authentication information: decrypt token fail",
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

可能原因

用户的API所属IAM认证，TOKEN解析失败。

解决办法

- 检查获取token的方法，token是否正确。
- 检查获取token的环境与调用的环境是否一致。

Incorrect IAM authentication information: Get secretKey failed

```
{
"error_msg": "Incorrect IAM authentication information: Get secretKey failed,ak:******,err:ak not exist",
"error_code": "APIG.0301",
"request_id": "******"
}
```

可能原因

用户的API所属IAM认证，使用AK/SK签名方式访问，但是AK不存在。

解决方法

检查AK填写是否正确。

14.5 API 控制策略

14.5.1 API 流量控制

14.5.1.1 是否支持对请求并发次数做自定义控制?

不支持。流控策略只控制单位时间内调用次数，无请求并发次数控制。

14.5.1.2 每个子域名（调试域名）每天最多可以访问 1000 次，如果帐号为企业帐号，是否还有这个限制?

每个子域名每天最多可以访问1000次的限制同样适用于企业帐号。

14.5.1.3 API 调用是否存在带宽限制

专享版API网关存在带宽限制，在创建实例时可以选择公网入口以及出口带宽。

14.5.1.4 流量控制策略不生效怎么办?

若流控策略的API流量限制或源IP流量限制不生效，检查API是否绑定流控策略。

若流控策略的用户流量限制不生效，检查API的安全认证方式是否为APP认证或IAM认证。

若流控策略的凭据流量限制不生效，检查API的安全认证方式是否为APP认证。

14.5.2 API 访问控制

14.5.2.1 怎样给指定的用户开放 API

可以采用以下两种方式：

- 创建API时可选取APP认证方式，APP key和APP Secret分享给指定的用户。
- 使用访问控制策略，按照IP地址或者帐号名，只允许符合允许策略的用户调用API。

14.5.2.2 配置了身份认证的 API，如何在特殊场景下（如指定 IP 地址）允许不校验身份?

认证方式不能基于某个特殊场景进行选择性认证。

- 方案1：创建API时选择无认证方式，然后利用“访问控制策略”功能进行IP白名单过滤，使得所有调用都不需要校验身份。
- 方案2：考虑拆分成2个API，其中一个使用身份认证（IAM认证或APP认证），另一个使用“无认证”并设置访问控制策略，以确保安全。

14.6 API 发布

14.6.1 对 API 的修改是否需要重新发布?

API发布后，如果再次编辑API参数，需要重新发布才能将修改后的信息同步到环境中。

14.6.2 API 发布到 RELEASE 环境可以正常访问，发布到非 RELEASE 环境无法访问?

添加x-stage请求消息头后即可访问。

例如：

```
r.Header.Add("x-stage", "RELEASE")
```

14.6.3 API 发布到不同环境后，会调用不同的后端服务吗?

使用环境变量，或者在后端服务定义不同的参数，可以实现API发布到不同环境时，调用不同的后端服务。

14.6.4 API 调试的时候，如何指定环境?

不能指定。API控制台提供的调试功能，用的是特定的debug环境，调试完成后需先发布到对应环境，之后可使用代码或者postman等工具，并添加请求消息头X-Stage，才能访问指定环境。

14.7 API 导入导出

14.7.1 API 导入失败是什么原因?

可能原因1：单次导入的API数量超出上限。当前单次最高能导入300个API，如超出此数量，请分批导入，或提交配额修改工单，调整API单次导入上限。

可能原因2：参数错误，需要检查和修正。建议先在API网关控制台界面创建一个API，将其导出作为API文件的模板。

可能原因3：YAML文件格式问题，需要检查和修正。

可能原因4：本地proxy网络限制，更换网络环境。

可能原因5：定义API请求中，不允许在Header定义“X-Auth-Token”字段。

14.7.2 swagger 导入 API 的扩展字段有没有模板?

模板在开发中。

您可以先配置好1~2个API，再导出作为模板。

14.8 API 安全

14.8.1 怎样保护 API?

- 使用身份认证

  创建API时，为API调用增加身份认证，如使用IAM认证或API网关提供的APP认证，防止API被恶意调用。

- 设置访问控制策略

  从IP地址（或地址区间）以及帐号等不同维度，设置白名单/黑名单。

- 将API绑定流控策略，通过流控策略保护API。

  API网关默认API流量控制为每秒200次，如果您的后端服务不能支撑单个API 200次/秒的调用请求，可设置流量控制策略，将限额调低。

14.8.2 怎样保证 API 网关调用后端服务器的安全?

通过以下方法确保API网关调用后端服务器的安全：

- 为API绑定签名密钥。

  在绑定签名密钥后，API网关到后端服务的请求增加签名信息，后端服务收到请求后计算签名信息，验证计算后的签名信息与API网关的签名信息是否一致。

- 使用HTTPS对请求进行加密。

  需要确保已有相应的SSL证书。

- 使用后端认证：

  您可以对后端服务开启安全认证，只受理携带正确授权信息的API请求。在创建API的定义后端服务阶段，可以开启后端认证。

14.8.3 能否针对 VPC 通道（负载通道）内的 ECS 私有 IP 进行访问控制

不支持。

14.9 其他

14.9.1 API、环境、凭据之间的关系?

API可以被发布到不同的环境中。比如RELEASE和BETA两个环境，分别代表线上和测试环境。

凭据指代一个API调用者的身份。创建凭据时，系统会自动生成用于认证该身份的凭据key&secret。将指定的API授权给指定凭据后，该凭据的持有者才可以调用已发布到环境中的指定API。

同一个API发布到不同的环境时，可以为之定义不同的流控策略并授权给不同的凭据。举例，API v2版本在测试过程中，可以发布到BETA环境，并授权给测试凭据，而API v1版本是稳定版本，可以在RELEASE环境中，授权给所有用户或凭据使用。

14.9.2 怎样使用 API 网关?

API网关提供了以下方式来管理/调用API：

- Web化的服务管理平台，即管理控制台。

  如果您已注册云服务，可直接登录管理控制台，单击管理控制台左上角 ☰ ，然后单击“API网关 APIG”。

  有关管理控制台的功能描述以及操作使用指导，请参考《 API网关用户指南 》。

- 基于Java、Go、Python、Javascript、C#、PHP、C++、C、Android等多种语言的SDK包。

  您可以通过下载SDK包来调用API，具体操作请参考《 API网关开发指南 》。

14.9.3 API 网关支持哪些 SDK 语言?

API网关当前支持Java、Go、Python、C#、javascript、PHP、C++、C和Android的SDK。

14.9.4 API 网关是否支持通过 POST 方法上传文件?

API网关支持通过POST方法上传文件。

专享版：在实例配置参数中，配置“request_body_size”参数。“request_body_size”表示API请求中允许携带的Body大小上限，支持修改范围1~9536 M。

说明

目前仅支持对请求体透传。

14.9.5 如何获取 API 网关错误返回信息?

当API请求到达网关后，网关返回请求结果信息。查看返回结果的Body信息如下。

```
{
    "error_code": "APIG.0101",
    "error_msg": "API not exist or not published to environment",
    "request_id": "acbc548ac6f2a0dbdb9e3518a7c0ff84"
}
```

- “error_code”表示错误码。
- “error_msg”表示报错原因。

14.9.6 API 网关是否支持部署到本地?

目前不支持API网关部署到本地。

15 修订记录

表 15-1 文档修订记录

发布日期	修订记录
2023-05-30	本次变更： **调用API**新增“使用IP调用非DEFAULT分组的API”。
2023-04-30	本次变更： ● 用户指南全量更新。 ● 产品介绍和常见问题应用更名为凭据，VPC通道更名为负载通道等，新旧UI差异见**新旧版本差异**。
2023-03-30	本次变更如下： ● 新增**产品规格差异**章节。 ● “简介”章节更名为“APIG使用流程”，并更新内容。
2022-10-30	本次变更如下： ● 新增**产品介绍**。 ● 新增**权限管理**。 ● 常见问题新增**IAM认证信息错误**、**部署在VPC下的应用是否可以调用API？**、**新建一个IAM认证方式的API，在配置入参时为什么无法配置HEADER位置的x-auth-token？**、**为什么分组跨域配置失败？**。
2022-07-30	第二次正式发布。 ● **创建API**定义后端服务为functiongraph时，支持别名选择。 ● API网关支持**支持HTTP2.0**。
2020-11-05	第一次正式发布。